UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

EL IMPACTO DE LA VIGILANCIA MASIVA Y ESPIONAJE A TRAVÉS DE NUEVOS MECANISMOS EN LAS RELACIONES INTERNACIONALES

TESIS

QUE PARA OBTENER EL TÍTULO DE
LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTA:
KARLA MARÍA SALINAS GARCÍA

DRA. SANDRA KANETY ZAVALETA HERNÁNDEZ

CIUDAD UNIVERSITARIA, CD.MX. 2023.

Agradecimientos

Por todos los años, el tiempo, el esfuerzo, el trabajo, la dedicación, el desvelo, los gastos, la perseverancia, la tolerancia a la frustración, las ganas y el desgano, los tropiezos, la edad, las caídas y levantadas.

Por las muchas ganas de hacerlo y los pocos recursos para hacerlo, en un acto de completo egoísmo, le dedico esta tesis a:

Karla María Salinas García

Gracias por todo, se logró el objetivo y me siento orgullosa del resultado.

No sin antes mencionar a las personas que estuvieron ahí para levantarme cuando caía y a darme ánimos para llegar aquí.

Gracias infinitas a mi mami María de la Luz García Suárez, que siempre es la más orgullosa de mí, con su apoyo incondicional y motivación sin medida, es mi regalo para ella.

A mi hermanos.

A mi asesora la Dra. Sandra Kanety que desde que la conozco, nunca ha dejado de creer en mí, de apoyarme, dirigirme y siempre estar al frente conmigo.

A la Universidad Nacional Autónoma de México y a la FCPyS que siempre me ha dado todo para continuar y crecer, por darme alas para volar alto.

A mi señor padre por el apoyo económico durante mis estudios.

A Héctor Pérez Ibarra por ser siempre la luz al final de mi negativo camino.

Y a todas las personas que algún día confiaron en que esto… terminaría.

C'est fini.

Índice

El Impacto De La Vigilancia Masiva Y Espionaje A Través De Nuevos Mecanismos En Las Relaciones Internacionales

Introducción

> El espionaje electrónico masivo y el uso de drones armados representan prácticas que ponen en peligro los derechos humanos en el planeta… si bien las nuevas tecnologías transforman de manera positiva la vida de las personas, son utilizadas para afectarla y ponerla en peligro… la ley internacional, la vigilancia masiva electrónica y la recolección de informaciones amenazan tanto las libertades individuales como el funcionamiento libre de la sociedad civil.
>
> Navi Pillay
> Alta Comisionada de la ONU para los Derechos Humanos

Para poder comprender un poco la normalización de la vigilancia social, es necesario entender a las sociedades en el siglo XXI, mismas que sufren y son afectadas por lógicas económicas, políticas y culturales que parecieran no tener ningún límite normativo, además de políticas públicas penales, de espionaje y controles sociales a partir de contextos extremadamente violentos, como negocios de tráfico de armas, drogas y formas de militarización en relación a ello, lo cual tiene como consecuencia, afectaciones en comunidades y sus formas de vida, principalmente en grupos vulnerables.

Otras lógicas de exclusión son la acumulación económica con su consecuente explotación laboral, marginación de amplios grupos poblacionales, que son también parte de este circuito de excepcionalidad o Estado de excepción, tal como lo llamaría Giorgio Agamben y que se menciona en este documento. Se puede decir que, los efectos en torno a las expectativas sobre la seguridad son parte de los procesos psicosociales que en condiciones de Estado de excepción fundamentan el aparato y promueven funciones de la política como el control social. Las anatomías de poder vigentes relacionan el control y la vigilancia aceptándolas en la cotidianidad, por ejemplo; el sistema de vigilancia como las cámaras instaladas en la ciudad y que dotan de un sentido de seguridad, así como el conocimiento de las rutas, horarios y afectos que los dispositivos facilitan a los mecanismos modernos.

Si tuviéramos que ponerle un nombre a este sistema de vigilancia en particular, se le nombra y se le conoce actualmente como “el internet de las cosas que consiste en que las “cosas” tengan conexión al Internet en cualquier momento y lugar aparatos tales como un teléfono, una computadora o una Tablet. En un sentido más técnico, consiste en la

integración de sensores y dispositivos en objetos cotidianos que quedan conectados a Internet a través de redes fijas e inalámbricas"[1]. Como bien se menciona, el objetivo de este enfoque es conocer o en su caso, explicar que el internet está presente todo el tiempo y de manera constante en nuestra cotidianidad y que el impacto que tiene este tipo de vigilancia es el que recae sobre la sociedad, la economía, la política, los negocios entre muchas otras áreas sociales. Que, si bien este sistema no se da únicamente por el internet de las cosas, e busca reflejar la situación actual de la privacidad, vigilancia y espionaje a través del mismo.

Algunos de los objetivos de este trabajo buscan explicar la tensión que se ha provocado entre el orden y el ejercicio de control social por parte de las instituciones estatales y conocer el proceso de vigilancia basado en el mecanismo de poder sin dejar de aclarar que los artículos comentados per se no provocan violencia ya que la violencia es una relación social, es decir, es una relación que actúa entre sujetos, entre humanos. Para ser más claros, un dron, una pistola o una aplicación no es violenta por sí misma, es un medio para ejercer un acto violento, para ejercer una conducta de violencia sobre otra persona o grupo con el objetivo de cumplir los intereses personales, al final del día son dispositivos tecnológicos que ayudan a mantener un orden social establecido, mismo que es estructuralmente violento y necesita de la violencia como forma relacional para seguirse manteniendo.

Esto se refleja también, en la desconfianza proveniente de la vigilancia como mecanismo de control, fundamenta regímenes autoritarios basados en el poder como dominio de todo proceso. Ante ello se mantienen condiciones de explotación económica, opresión cultural, discriminación identitaria y dominación política. Lo cual, afecta sobre todo a grupos vulnerables considerados incapaces de autogobernarse, dictaminando políticas dirigidas a controlar sus cuerpos y sus devenires, consolidando un espacio de poder estatal cerrado y de vigilancia a quién entra y sale, ya que de cierta manera, aprenden a espiar, a desconfiar, a mirar con ojos inquisitivos, a prejuzgar sin razón, a determinar a una persona por su apariencia, a alterar a través del espionaje los cursos de una sociedad o a interferir en un país para beneficio económico de grandes potencias.

Con base en los análisis realizados, alimentar las condiciones de vigilancia genera que se internalice la represión, que se legalice el castigo policial, que se dote de autonomía a los cuerpos policiacos y otros grupos que surgen para castigar a los criminales sin código

[1] El *internet* de las cosas. [En línea]. http://boletines.prisadigital.com/El_*internet*_de_las_cosas.pdf. [Página consultada el 29/III/2020].

legal sino desde la estigmatización. Ante ello, se considera que, la respuesta histórica a la necesidad de controlar a los grupos sociales que deviene en sistemas punitivos que sofistican la vigilancia y el castigo ejemplar, sólo provocan más violencia.

El proceso social de agenciamiento a dichas lógicas de vigilancia es preocupante por la desconfianza que se genera no sólo a las instituciones del Estado sino a las propias personas de cualquier comunidad, lo cual incide en la desarticulación que pudiera promover el ejercicio de los derechos civiles, políticos y sociales, toda vez que el Estado no pueda ser capaz de controlar las dinámicas humanas y es necesaria la relación civil, económica y política entre individuos conscientes de su aporte en la red social.

El desarrollo de nuevas tecnologías de vigilancia aplicadas a la vida diaria, incrementan las formas neoliberales de descobijamiento de la ciudadanía frente a sujetos corporativos que insisten en lógicas beligerantes, permitiendo implementar tecnologías de la vigilancia internacional y de espionaje en las cotidianidades. De esta manera, las políticas públicas y las instituciones que las arropan tienden a mantener y garantizar dichas dinámicas tanto por sus omisiones y silencios como por desconocimiento del tema, provocando la desconfianza de la sociedad sobre las evidentes ausencias y anomias que genera este circuito.

Es por eso que, uno de los objetivos de este trabajo, será conocer y dotar de información sobre la estructura de la seguridad internacional investigando también el papel fundamental que juegan las redes de información actuales ante el uso de la tecnología además de, conocer los sistemas modernos de vigilancia y los flujos de información que tienen sobre los individuos.

Además, la investigación académica es fundamental para proveer recursos teóricos y análisis objetivos que puedan conocer del nivel de intervención que se ejecuta en las vidas personales y en la de las sociedades, a través de los dispositivos tecnológicos que utilizamos día a día. El tema gira en torno a visibilizar los dispositivos de vigilancia y las relaciones de poder que sustentan en su nivel internacional así, como analizar sus usos.

Por ende, el tema versa sobre la vulnerabilidad que provoca el mantener ciclos de control en contextos donde la violencia se normaliza, en lugar de democratizar las formas de acceso económicas, políticas y culturales, así como las relaciones internacionales, en el entredicho de hacer frente a las posiciones recalcitrantes que acumulan poder y riqueza en un mundo de grandes desigualdades.

Por lo cual, la presente investigación consta de cuatro capítulos, el primero hace referencia a los primeros rasgos de espionaje registrados en la historia del mundo ya sea

mediante el espionaje Internacional con sucesos como guerras y ataques internacionales que han legitimado una nueva era de vigilancia global y cercamiento a ultranza de las fronteras.

Dando paso a une legitimación de la vigilancia durante el Siglo XXI cuando se puede observar a detalle una evolución en la misma que da para adelantos basados en la estigmatización de las personas bajo el estereotipo de terroristas y sus implicaciones con las políticas migratorias, fronterizas y de seguridad actuales afectando así las garantías individuales y los Derechos Humanos de la sociedad dejando como consecuencia un impacto en la forma de violencia estructural misma por la que las Organizaciones No Gubernamentales y grupos interesados tratan y buscan la creación de legislaciones o regulaciones en torno a estos temas sin fetichizar la tecnología.

Así, se da paso al segundo capítulo en el que se analiza el entorno e historia de los mecanismos y dispositivos de vigilancia tales como los drones, las aplicaciones, cámaras de seguridad y demás aparatos que tecnológicamente ayudan a mantener el orden que es estructuralmente violento exponiendo así la tensión que se ha provocado entre el orden y el ejercicio de control social por parte de las instituciones estatales, lo que supone una realidad inquietante en el ámbito social, pues se considera que, desde esta multiplicidad entre organismos de gobierno y mecanismos de control se ha creado y ejercido la vigilancia en las redes sociales en la cual se ha quedado atrapada la sociedad y que hasta hoy día no se tiene la noción de si estas están delimitadas o tienen condiciones establecidas, algunas normas, instructivos o leyes.

Aprovechando de esta manera, el análisis a WikiLeaks como instrumento tecnológico utilizado en contra de los gobiernos por la inexistencia de normas o regulaciones provocando así filtraciones de información que han resultado sumamente importantes no solo para la sociedad, política y cultura de los Estados Unidos sino también de otros países involucrados en los mismos.

Dando pie al tercer capítulo, enfocado en algunos de los casos que han sido públicamente destapados en lo que se utilizan herramientas tecnológicas para espiar, rastrar y tener información de personas, gobiernos y Organizaciones No Gubernamentales tal es el caso de Snowden, Operación Aurora y Caso Echelon.

Compartiendo así el capitulo con un par de casos mexicanos en los que el gobierno de Enrique Peña Nieto se vio involucrado al hacerse acreedor de noticias de espionaje como el caso de Pegasus y Caso Aristegui espiando a reporteros a través de malware contratados con dinero público a gobiernos de Medio Oriente. Por último, pero no menos

importante, se compartirá un caso práctico con resultados resumidos en gráficas sobre la percepción de la sociedad antes estos casos y sus nulas o inexistentes normativas, mismas que dan pie a un análisis que profundiza en la situación actual en cuánto a las formas de violencia estructural y conocimiento de las mismas.

Continuando con el trabajo, debe tomarse en cuenta que, la categoría de espionaje en el Derecho Internacional ya no abarca la multiplicidad de usos y dispositivos que sirven para infiltrar y penetrar en la información estratégica de gobiernos y empresas o individuos con liderazgo social. Para lograr la investigación, se responderán algunas preguntas tales como:

¿Puede considerarse invasión de privacidad, uso de datos personales sin autorización, intervención ilegal en las comunicaciones, espionaje de personas, uso de información para lograr objetivos en contra de individuos, entre otros cómo prácticas de vigilancia?

¿Hacia dónde evoluciona la categoría de espionaje si se normalizan estas prácticas de vigilancia o infiltración?

¿En qué medida la vigilancia proporciona medios para mantener sociedades controladas?

Hasta ahora, la tecnología y la creciente necesidad social de comunicación, ha destapado una nueva era de vigilancia, misma que comienza rígida y abiertamente a partir del de los acontecimientos del 11 de septiembre de 2001, situación que legitimó la persecución basada en la estigmatización de las personas bajo el estereotipo de terrorista y sus implicaciones en las políticas migratorias, fronterizas y de seguridad en todo el mundo.

En esta investigación, se mencionan distintos tipos de vigilancia internacional que van desde los métodos más antiguos como los drones, mismos que son clasificados como tal, hasta los más nuevos y actuales tales como los malware y el uso de las aplicaciones que son cotidianas en nuestras vidas. La situación de espionaje y vigilancia será abordada con base en la ideología de uno de los filósofos más importantes y relevantes en cuanto al tema, Foucault dará las bases para el análisis social de los temas que se trabajan en este trabajo.

La hipótesis relacionada con la problemática es que el espionaje generalizado es de conocimiento público y se han detectado cada vez más interferencias en personas consideradas peligrosas para determinados grupos en el poder, aunque ya se han usado diversas tecnologías para la vigilancia militar desde Vietnam hasta Centroamérica, mientras que se legitima su uso actual en México, dentro del propio Estados Unidos, y otros países

y contra personas para inculpar y sostener versiones ilegales lo cual genera violencia estatal.

Grupos de poder y de inteligencia militar en Estados Unidos y otras potencias, obtienen información y las posibilidades para regular, limitar o contener ese poder-saber que los dota de una ventaja abismal por sobre otros países sin la suficiente tecnología, y terminan por orientar y conducir hacia intereses extranjeros a las naciones sin dicha capacidad.

Los testimonios, artículos relevantes, guías y demás están fundamentados por la lectura y revisión de artículos, tesis, capítulos de libros o informes internacionales relacionados con las categorías de vigilancia, castigo, espionaje, control social, sociedad de control, sociedad disciplinaria, violencia de estado, entre otros.

Desde el punto de vista de lo tecnológico, se hará una revisión en lo que existe sobre dispositivos militares y su historia, en bibliotecas, web y entrevistas con especialistas. Sobre el contexto social del espionaje en el ámbito Internacional se involucran archivos, Informes, Protocolos, Declaraciones, Conferencias y Casos en la materia.

Por último, también se hace hincapié en la infiltración de información estratégica de gobiernos y empresas o individuos con liderazgo social, se indagará en la información en prensa, redes sociales, organizaciones de la sociedad civil dedicadas al tema. El caso de México es particularmente interesante ya que si comenzamos con el inicio de la nueva vigilancia podemos hablar de los drones, mismos que han sido utilizados por grupos de narcotraficantes y delincuencia armada para intereses personales y económicos. Además de que es importante mencionar que el uso de vigilancia o grabación no consentida sobre población carece de normativas y pueden ser utilizados de manera privada y sin ninguna restricción.

Por otro lado, han ayudado en causas sociales para dar cuenta de apresamientos ilegales y en condiciones inadecuadas de personas inocentes frente a los cuerpos policiacos. Si algo tienen en común los sistemas modernos de vigilancia es la multiplicidad de flujos de información que contiene, por la comunicación generalizada y “libertad” del sistema en general. Paradójicamente, estas libertades de comunicación y expresión que se solicitan a las sociedades democráticas también son requeridos por poderes fácticos dentro del estado, cuando hay conflicto de intereses entre pueblos o comunidades e intereses económicos.

En las últimas décadas, el avance que ha tenido la tecnología a través del ámbito internacional ha sido completamente notorio y significativo socialmente lo que se ha

representado al mismo tiempo como una solución ya que se mantiene interconectado y experimenta al mismo tiempo una flexibilidad para el espionaje.

Mismo espionaje que se dirige y se concentra en la manipulación de información en cuánto a temas de inseguridad ya que es de conocimiento público que estos nuevos sistemas han afectado profundamente a las relaciones internacionales, interpersonales e institucionales. Los avances diarios en estas tecnologías de la información y de vigilancia ocasionan que se tengan un sinfín de oportunidades y ventanas abiertas a la información privada ya sea de cualquier individuo o de cualquier ente privado como gobiernos, organizaciones, y organismos.

Tras los hechos del 11S "la Agencia de Seguridad Nacional de Estados Unidos desarrolló nuevas funciones para la evolución tecnológica al servicio de su país y que precisa en contar con un amplio entramado de industrias, universidades y redes de apoyo que pretenden vigilar a todo lo que pueda afectar a los intereses de seguridad"[2].

A pesar de las intervenciones de mecanismos reguladores internacionales como la ONU en temas sobre el cuidado de la información privada y espionaje, está claro que la sociedad ya sea internacional, política, privada o individual ha sido vulnerada ya que, en cualquier momento, la información "personal" puede ser de dominio público y al tiempo utilizada como ventaja para los intereses de quienes la tienen en su poder.

[2] Espionaje y seguridad en las redes. [En línea]. https://es.slideshare.net/LauDiaz05/espionaje-y-seguridad-en-las-redes. [Página consultada el 08/III/2021].

1. RASGOS DEL ESPIONAJE Y LA VIGILANCIA INTERNACIONAL

> Uno asumiría que en un país tan tranquilo como lo era México hace algunos años, lo más cerca que estábamos del espionaje era asistir a ver una película del agente 007, pero esto no era cierto, México ha sido uno de los campos de batalla principales en las guerras de espionaje de los últimos dos siglos, particularmente durante la guerra fría.
>
> Sergio Antonio Téllez Morales

1.1. Antecedentes de la institucionalización del espionaje

Es casi imposible afirmar que, las primeras manifestaciones de la utilización de los servicios de inteligencia y de espionaje se remontan a Mesopotamia en el III milenio a.C., sin embargo, existen evidencias de cuando Sargón I de Acad se hizo con el poder, reuniendo bajo su cetro un imperio que abarcaba desde las costas de Siria hasta el sur del actual Irán. Otra gran referencia es la relacionada con los espías a las órdenes de Hammurabi, el que fuera rey de Babilonia entre 1792 y 1750 a. C., mismos que intentaban conseguir información infiltrándose en el ejército de Zimri-Lim y así minar los planes de sus comandantes. Sin embargo, como cita Herrera,

"Aunque la utilización de la inteligencia militar se dio en todas las civilizaciones antiguas, será en el Imperio chino donde encontremos el primer tratado militar en el que se hace referencia al espionaje: el Arte de la guerra, de Sun Tzu"[3].

Pero hay que reconocer que, si bien Sun Tzu es el teorizador del arte de la guerra y de la inteligencia aplicada al combate que más importancia ha tenido en la posteridad, no es el único gran pensador sobre el espionaje que ha dado la Antigüedad, pues en la antigua India, tras la muerte de Alejandro Magno en el 323 a. C., el rey indio Chandragupta Maurya (c. 317-293 a. C.) empezó la conquista de tan vasto territorio contando con el apoyo de uno de los más grandes estrategas de la Antigüedad, su consejero Chanakya, también llamado Kautilya, conocido como el Maquiavelo de la India[4]. "Considérese que, para Herrera, tanto pasajes de la Biblia, como de Grecia y Roma están saturados de anécdotas de espionaje,

[3] Juan Carlos Herrera Hermosilla. *Breve historia del espionaje*. Ediciones Nowtilus, S.L. Madrid, España, 25 pp.

[4] Oscar Álvarez Araya. [En línea]. https://wsimag.com/es/cultura/62465-chanakya-el-maquiavelo-de-la-india. [Página consultada el 29/V/2019].

llegando a afirmar este autor que “ningún imperio desde la Antigüedad se ha forjado sin la utilización del espionaje”[5].

Por su parte, Pablo Jarabo Valdivieso recurre a dividir los antecedentes del espionaje en cuatro etapas, a saber: la Edad Antigua; la Edad Media, la Edad Moderna y la Era Contemporánea, puestas en la Tabla 1 (elaboración propia con información de Pablo Jarabo Valdivieso).

Tabla 1. Historia y evolución del espionaje

Época	Acontecimientos
Edad Antigua	- Mesopotamia registra en el III milenio a.C. las primeras muestras de la utilización de los servicios de inteligencia y espionaje, en el reinado de Sargón I de Acad. - Un testimonio lo es una tablilla escrita en acadio con caracteres cuneiformes, fechada hacia el 2210 a. C., en la que se aprecia cómo Argón I se servía de mercaderes para que le proporcionasen información sobre las poblaciones que quería conquistar. - En Grecia, en la obra de Homero, la Ilíada, ya se habla del espionaje utilizado en la guerra de Troya. - Historiadores como Tito Livio y Sexto Julio Frontino (300 a.C.) han señalado que, en Roma el espionaje era muy utilizado.
Edad Media	- El espionaje puramente militar se practicó en contiendas como la de Ad Decimum (533 d.C.) y la de Hastings (1066 d.C.). - En Extremo Oriente el espionaje militar fue practicado por exploradores y guerreros espías, como Gengis Kan. - En el Japón medieval durante la etapa Sengoku (1467-1568), surgieron dos nuevos tipos de guerreros: los samuráis, que representaban el valor ancestral del honor en la guerra; y los ninjas, también llamados *shinobi*, considerados guerreros espías.
Edad Moderna	- El imperio británico fue el primero en crear una red de inteligencia institucionalizada. Esto fue llevado a cabo por el secretario de Estado de Isabel I, sir Francis Walsingham, que desarrolló tal cometido de 1573 a 1590. - El imperio español estableció, a manos de Felipe II, una gran red de espionaje cuyos centros de operaciones eran las embajadas. - Francia y Rusia formaron sus propias redes de espionaje tanto interno como externo, al participar de manera directa en el ámbito de las operaciones secretas de la política mundial.
Era Contemporánea	- La antesala de la 1º Guerra Mundial y el ambiente bélico que se respira en Europa a finales del siglo XIX y principios del siglo XX hará que se extienda la utilización de las redes de inteligencia de manera global por todo el mundo. - Se ponen al servicio de los espías los avances tecnológicos, tanto los ya existentes – fotografía, telégrafo o teléfono– como los de más reciente aparición, el telégrafo. - En toda Europa surge una gran obsesión por el espionaje.

[5]Juan Carlos Herrera Hermosilla. *Ibid*, p. 42

	- El paulatino alejamiento de las relaciones políticas entre Gran Bretaña y el imperio alemán y la disposición beligerante de este último llevaron al imperio británico a fundar en, octubre de 1909, de la mano de William Melville, superintendente de Scotland Yard, el *Secret Service Bureau*, es decir la Oficina del Servicio Secreto, donde se aglutinan los diecinueve departamentos de la inteligencia militar, conocidos con las siglas que van desde el MI-1 al MI-19. Los más famosos son el MI-5, dedicado a la seguridad interna, es decir, al contraespionaje, y el MI-6, encargado de la seguridad externa, esto es, el espionaje en el extranjero. - En 1908, en los Estados Unidos de Norteamérica, se crea una Oficina de Investigación que después se convertiría en el FBI. - En la Segunda Guerra Mundial resalta la *Operación Fortitude*, en la que el espía español Juan Pujol García, al servicio de la inteligencia británica, logró engañar al ejército alemán facilitando falsa información sobre el desembarco aliado en Normandía, afirmando que este se produciría las costas de Calais. - Surgen los espías atómicos, encargados de recabar toda la información posible acerca de los avances técnicos que se produjesen en relación con la tecnología atómica. - En la Alemania nazi, existió un cuerpo de policía dirigido por el general Himmler, que estructuró una red de espionaje cuyo objetivo eran los detractores del régimen y los que consideraban *impuros.* - Durante la Guerra Fría, los dos países que representaban los bloques enfrentados: el capitalista encabezado por los Estados Unidos; y el comunista, por la URSS, infiltraron agentes para obtener información secreta relativa a la estrategia y la tecnología, hasta convertirse en una obsesión por creer tener al enemigo dentro del país. - Lo anterior, dio lugar al surgimiento de la CIA (Agencia Central de Inteligencia) en EE.UU. y la KGB (Comité para la Seguridad del Estado) en la URSS. - Durante la década de los setenta, los métodos usados en el ámbito militar, como vigilancia exhaustiva, pinchar teléfonos, escuchas ilegales… pasan al ámbito político, lo que se conoce como espionaje político. Así ocurrió en el caso más famoso a nivel mundial de toda la historia: el caso Watergate

Tabla de elaboración propia con información de: Pablo Valdivieso. *El Espionaje. Pasado y Presente.* [En línea]. https://apavaldeluz.files.wordpress.com/2015/05/el-espionaje-pablo-jarabodef.pdf. [Página consultada el 29/V/2019].

Otro interesante argumento acerca de los antecedentes del espionaje es el que hace Thomas Sepúlveda Whittle (1936), el cual refiere que, un espía

"Es un héroe anónimo que expone su vida minuta a minuto de su existencia, que renuncia a su tranquilidad personal, que sacrifica su serenidad de espíritu, y que aún pasa por encima de los escrúpulos y vence a sus propios instintos, para luchar con todas las fuerzas de su inteligencia por los altos intereses de su Patria"[6].

[6]Whittle Sepúlveda. *Espionaje y Contra-Espionaje*. [En línea]. http://agenciabk.net/espionajecontra.pdf. (p.9). [Página consultada el 20/V/2019].

Cabe señalar que, para Sepúlveda, los también llamados agentes secretos se pueden clasificar de la siguiente manera:

a) **"Espías por Patriotismo Puro**. Ejemplo de ello son el teniente de la Marina Imperial Alemana, Cari Hans Lody, condenado en 1914 a largos años de reclusión y el Capitán Yon Eintelen, que sólo pudo regresar a Alemania en 1921, después de haber permanecido preso en Estados Unidos durante cuatro años. Otra referencia es el Capitán Trench, de la Marina Británica, parte del *Intelligence Service*, el cual actuó en Alemania en 1913 y logró obtener, entre otros documentos de importancia, fotografías de los planos del Crucero Yan der Tann y del Código de Señales de la Escuadra Alemana, escapando de la policía en forma espectacular.

b) **Espías por dinero, (incluyendo necesitados y aventureras)**. Entre los espías a sueldo, está el espía-policía de la Guerra Europea, Charles Lucieto. Otro caso es el del ministro de Guerra Ruso, Soukhumlinov, el cual se vendió a Alemania, y después de haber causado con su política anti-patriota y con sus informes, miles de víctimas entre sus connacionales, argumentó que tenía una mujer muy gastadora, a quien debía proporcionar pieles riquísimas y piedras preciosas.

c) **Traidores**. Aquí, cabe nombrar a Ignatius Thimotey Trebisch-Lincoln, nacido en Hungría, de origen judío. Se trasladó a Inglaterra, donde fue sucesivamente, católico, anglicano, y pastor de la Secta Baptista, y, habiéndose nacionalizado ciudadano británico, ingresó al Partido Liberal, por el cual, gracias a su astucia y a sus intrigas, llegó a ser Miembro del Parlamento Británico. Se enroló en el *British Intelligence Service*, insistiendo en querer pertenecer a este organismo, con el pretexto de demostrar su cariño a Inglaterra, pero con la idea de trabajar en contra de ella. Antes de que pudiera desarrollar sus nefastos planes, fue descubierto, y se convirtió en Monje Budista. Otro caso es el del coronel Alfredo Redi, Jefe del Servicio de Informaciones del Estado Mayor General Austríaco, quien trabajaba a favor de Rusia, la enemiga natural de su país.

d) **Agentes Femeninos y Espías por Amor**. En este tipo, se puede referir a Miss Edith Cavell, que pagó con la vida su valiosa labor a favor de los heridos aliados, a quienes ayudaba a repatriarse después de cuidarlos en su hospital particular en Bélgica, y Martha Knockaert, más tarde Martha Me Kenna, una joven belga condecorada con la Cruz de Hierro Alemana por su abnegación en aliviar a los heridos. También, en la historia del espionaje de la Gran Guerra, abundan mujeres que practicaban este oficio por dinero, como el caso de la famosa bailarina Mata-Hari. Otras espías de amor lo son Mademoiselle Docteur, querida del Capitán Winanky, considerada la espía más completa de que haya memoria, y Ana Wittig, cuyo amor por el Conde Chilly, Oficial Francés del Servicio de Informaciones, la llevó a preparar y realizar la estrategia que sirvió para adquirir la certeza

de que Mata-Hari era espía alemana. Tiempo después, acosada por el remordimiento, se suicidó".[7]

Así, para resaltar la trascendencia del espionaje, Sepúlveda refiere las palabras del Capitán Ferdinand Tuohy el cual consideraba que sin un Servicio de Informaciones en el campo de batalla no se podría haber ganado la guerra, como no se podría haber triunfado sin los tanques o sin la aviación.

Como es lógico suponer, todos los acontecimientos citados alteraron el entorno o ambiente internacional, dando lugar a concepciones, enfoques y prácticas de vigilancia entre los más diversos países del orbe.

1.2. Entorno de la vigilancia y el espionaje

Sin duda alguna, la vigilancia se puede explicar como el enfoque que engloba las prácticas permitidas para el control de sujetos en el ámbito particular, público e íntimo. Utiliza una investigación teórica metodológica dentro de las Relaciones Internacionales y trata de comprender a las sociedades por medio de la vigilancia y el control mediante el modelo de Michael Foucault, el llamado teórico del poder quien trata de evidenciar la sociedad disciplinaria. Así, como parte de la modernidad, la vigilancia ha remontado como un término bajo el control y el encierro desde la perspectiva institucional. Es decir, la vigilancia es parte de una dinámica de la globalización.

Por su parte, Bauman, menciona que:

> La vigilancia líquida no es tanto una manera integral de definir la vigilancia como un medio de orientarnos y situar los cambios dentro de la vigilancia dentro de la fluida e inquietante modernidad actual (…) se ha difuminado especialmente en la esfera de consumo (…) se está ahora desplegando en unas formas inimaginables, respondiendo a la liquidez y reproduciéndola (…) presionada por las exigencias de la seguridad y pasada por el prisma de la insistente publicidad de las empresas de la tecnología[8].

Para el mismo Bauman: el modelo panóptico es bien visto desde la perspectiva de Foucault, esto, al entender a la sociedad como un reflejo del sistema en el que se encuentra, es decir, la sociedad puede integrarse a una disciplina, misma que el poder instala para así tener el control y la vigilancia además de tener la capacidad para definir conductas en la población, ya sea castigando o premiando el buen comportamiento.

---

[7] *Op. Cit.*
[8] Zygmunt Bauman y David Lyon. *Vigilancia líquida*. Paidós, Barcelona, 2013, p. 11.

Retomando nuevamente a Foucault, existen tres tesis principales de poder que emanan de una relación que tiene con el poder. La idea es que el poder siempre está en circulación, siempre se está debatiendo y pugnando siempre hay dominantes y dominados, siempre hay una pugna y en realidad estas formas de vigilancia responden a esta pugna entre la relación de los ya mencionados. La relación de poder no es estática, no tiene un camino de arriba a abajo, sino que siempre está en pugna.

En este sentido, la relación de poder no solo reprime sino es una violencia productiva existe en este modelo la represión al sujeto mismo que encuentra en los modelos represivos ciertas formas de autoafirmación, por ejemplo, la gente no necesariamente se siente más seguro con una cámara que nos observe todo el tiempo, pero cuando algún altercado sucede, lo primero es voltear a ver las cámaras, mismas que si no están en el sitio, seguramente habrá una en corto tiempo debido al evento.

El conceso de la vigilancia continua, es algo que normalmente y conscientemente suele molestar de alguna manera a la sociedad, sin embargo, es aquí cuando la relación de poder no solo reprime sino también produce nuevas conductas y necesidad sociales hasta que se vuelven una necesidad. Las relaciones de poder entonces se construyen desde los mismos sujetos y no desde arriba hacía abajo todo el tiempo y por camino del estado sino desde una idea sociedad disciplinaria y panoptismo.

De alguna manera la sociedad ya acepta la vigilancia como un mecanismo legitimo de mantenimiento de normas y de esta manera, también las empresas y las organizaciones privadas que a través de las redes sociales generan ganancia a través de nuestra atención con elementos en los que nuestra privacidad está completamente vulnerada, misma que se refleja en una ganancia directa para estas empresas a través de hardware y software beneficiando sus intereses y vulnerando sociedad volviéndola mercancía.

Pero también, para el citado autor, a esta teoría se le puede integrar la categoría de banóptico, el cual se considera una práctica para vigilar que se nutre de las preocupaciones sociales, de la vigilancia actual y del desarrollo. A diferencia del Panóptico, esta teoría no ve necesario disciplinar; se puede decir, que se dedica a la inclusión y no a la exclusión[9].

[9] Si bien la teoría del panóptico se ha popularizado gracias a Michel Foucault, el concepto panóptico fue ideado por Jeremy Bentham como un mecanismo aplicable al control del comportamiento de los presos en las prisiones. El panóptico en sí es una forma de estructura arquitectónica diseñada para cárceles y prisiones**.** Dicha estructura suponía una disposición circular de las celdas en torno a un punto central, sin comunicación entre ellas y pudiendo ser el recluso observado desde el exterior. En el centro de la estructura se alzaría una torre de vigilancia donde una única persona podía visualizar todas las celdas, siendo capaz de controlar el comportamiento de todos los reclusos.

Con base en lo anterior se puede decir que, la vigilancia mezcla diferentes doctrinas para definir al ser humano como un peligro latente como, por ejemplo: los *guettos* de negros, los indígenas, los extranjeros, etc. De esta forma el individuo se vuelve adicto a la seguridad y dentro de su círculo cree necesario estar vigilado para sentirse protegido. Un ejemplo claro de ello es el miedo a los vecinos, a la gente de otro país, argumento que se centra en la adicción a la seguridad.

Pero ¿qué se debe entender por vigilancia? En opinión de Foucault:

> "Es un fenómeno a la vez individualizador y masificante, un aparato institucional dedicado a lograr el autodominio del sujeto y la sujeción, mientras se recaban todos los datos posibles que puedan hacerlo entrar en otro régimen de visibilidad. Este régimen es el biopolítico. Muchas veces se desconoce que el vínculo entre la anatomopolítica[10] y la biopolítica [11] se halla en este carácter bifronte de la vigilancia"[12].

Sin embargo, se puede decir que, en la actualidad, la vigilancia se basa esencialmente en la información tecnológica, más que en la información humana. El nuevo estado de vigilancia considera a cualquier individuo como sospechoso con el objetivo de que cualquier delito que se cometa sea reprimido inmediatamente. Sin embargo, las preguntas obligadas son: ¿qué se puede hacer? ¿cómo defenderse ante la invasión de privacidad? Ante esto, Whitaker refiere que:

"A pesar de que el espionaje es uno de los términos más antiguos de la historia, el mismo se ha convertido en una actividad burocrática, organizada y sistemática, con sus tecnologías específicas, su base de conocimientos científicos y su propio papel casi autónomo en la política nacional e internacional"[13].

Entonces, para Whitaker, uno de los pilares más importantes para realizar estas operaciones es el militar, aunado a que la evolución de los Estados se respalda en ella para convertirse en potencia y así demostrar no sólo a su sociedad sino a todos los demás su poder y evolución mediante cambios tecnológicos y de espionaje cuando es necesario. Es por eso que el control social que se ejerce actualmente es el que ha funcionado por todos los momentos de la historia, es decir siempre ha existido. Lo único que ha cambiado es la ideología y la manera de utilizarlo socialmente ya que se ejerce desde las redes y manipulación constante de los contenidos.

---

[10] Disciplina
[11] Población
[12] Pablo Rodríguez. *¿Qué son las sociedades de control?* [En línea]. http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf. [Página consultada el 8/VI/ 2019].
[13] Reg Whitaker. *El fin de la privacidad*. Paidós Comunicación, Barcelona, 1999, 16 pp.

Ahora, ¿qué entender por espionaje? Como definición se tiene la siguiente: “El espionaje es la actividad secreta que consiste en tratar de conseguir información confidencial, especialmente de un país extranjero[14].

Con la intención de contar con otro punto de vista, Navarro define al espionaje como:

> Toda acción perpetrada conscientemente para penetrar en un espacio informacional protegido o descuidado a fin de conseguir un incremento de conocimiento por medios encubiertos, insospechados o desconocidos por su legítimo productor o propietario. El espionaje busca de manera prioritaria la obtención de información no pública, protegida bajo diferentes niveles de clasificación y de accesibilidad muy limitada cuyo contenido es sensible y de alto valor para el conocimiento de capacidades e intenciones de un adversario, rival, enemigo o incluso aliado. El acceso no permitido y robo de esta información pone en riesgo al propietario de la misma generándole una vulnerabilidad en materia de seguridad nacional, en sus principios de bienestar social o en su posición competitiva en el marco de las relaciones internacionales[15].

Hay que considerar que, si bien existen múltiples definiciones, el espionaje consiste en una serie de acciones secretas para obtener cierto tipo de información. Cabe señalar que, existen varias técnicas de espionaje, explicadas por Alexandra Maldonado, a saber:

> **Infiltración.** Es la técnica utilizada para introducir unidades propias en las filas del contrario o blanco, para que suministren información de interés inmediato o potencial sobre las actividades, capacidades, planes, proyectos, etc. del contrario. También podría decirse que es la acción que consiste en la utilización de una persona, conocida como *topo*, cuyo cometido básico es ganarse la confianza de aquéllos que poseen la información para tener acceso a la misma.
>
> **Penetración.** Es la técnica que consiste en lograr la colaboración consciente o inocente de un miembro de la organización o grupo contrario con el fin de que proporcione datos e información confidencial del grupo al que pertenece. Generalmente, esta actividad se realiza de forma encubierta y emplea personas reclutadas que han sido persuadidas para trabajar en secreto en contra de su propia

[14]The Free Dictionary. *Espionaje definición*. [En línea]. http://es.thefreedictionary.com/espionaje [Página consultada el 08/ XI/ 2018]

[15]Diego Navarro Bonilla. *Espionaje, seguridad nacional y Relaciones Internacionales*. Colección de Estudios Internacionales, Bilbao, España, 2013, 10 pp.

> organización por diferentes motivaciones: ideológicas, económicas, morales, religiosas o personales[16].

Entonces, si bien el espionaje ha sido una de las prácticas más antiguas de la humanidad, en el caso de los Estados Unidos es hasta 1947 cuando surge lo que hoy se denomina Agencia Central de Inteligencia (CIA) por sus siglas en inglés, entre cuyos objetivos se encuentra.

> Recolectar información de inteligencia a través de fuentes humanas, y por otros medios apropiados; correlacionar y evaluar la inteligencia relacionada con la seguridad nacional y proveer la apropiada diseminación de tal inteligencia; proporciona dirección general y coordinar la recolección de inteligencia nacional fuera de los Estado Unidos a través de fuentes humanas de la Comunidad de Inteligencia autorizadas para realizar tal recolección, y realizar otras funciones y deberes relacionados a la inteligencia que afectan la seguridad nacional según instruya el Presidente o el Director Nacional de Inteligencia[17].

Ahora, para Whitaker, "hablar de servicios de inteligencia es clave mencionar que estos promueven los elevados costos de espionaje y es por ello que han contribuido a sustituir el trabajo humano por trabajo automático"[18].

Así, para este investigador, la interceptación de señales de comunicación, cuyas bases tecnológicas evolucionan a un ritmo exponencial, ha dotado a la escuela humana de unas extensiones deslumbrantes, pues como se sabe, en la actualidad, la mayoría de las comunicaciones auditivas pueden ser interceptadas por una serie de bases terrestres de escucha conectadas a una red local, como sucedió con la KGB, entre cuyas principales funciones se tenía: "Inteligencia exterior, contraespionaje, protección fronteriza, protección de los líderes del Partido Comunista y el Gobierno, el mantenimiento de las comunicaciones gubernamentales, la lucha contra el nacionalismo, la disidencia, el crimen y las actividades antisoviéticas"[19].

Considérese que, al término de la Guerra Fría, se encontró una cantidad excesiva de dinero invertido en el uso de satélites de espionaje y actualmente se lucha para que esos satélites sirvan para investigaciones y estudios en torno del medio ambiente.

---

[16] A. Maldonado Guanota. *Herramientas para evitar la infiltración y penetración en el ejército de Colombia*. http://repository.unimilitar.edu.co/bitstream/10654/7540/1/GuanotoaMaldonadoAlexandra2012.pdf. [Página consultada el 08/ XI/ 2018]

[17]Central Intelligence Agency US. *Acerca de la CIA*. [En línea]. https://www.cia.gov/es. [Página consultada el 08/ XI/ 2018].

[18] Reg Whitaker. *El fin de la privacidad*. *Ibidem,* 26 pp.

[19] KGB. [En línea]. https://actualidad.rt.com/actualidad/258012-rusia-celebrar-centenario-organos-seguridad-nacional. [Página consultada el 15/ XI/ 2018].

Ahora, parte determinante del entorno de la vigilancia y el espionaje fueron los hechos suscitados el 11 de septiembre de 2001 (11S), momento clave que replanteó la lucha contra el terrorismo, creándose nuevos programas de investigación que permiten filtrarse en la privacidad de la sociedad civil y todos los países del mundo. Cabe señalar que, el presupuesto planteado para estos programas asciende a los 52,600 millones de dólares cada año (con aumento gradual), información dada a conocer por Snowden.

Aunado a lo anterior, dentro de los programas que han sido creados contra el terrorismo, se sabe que:

> La Ley Patriota nace en octubre 2001. El Congreso aprueba y el presidente Bush la firma, esta ley amplía los poderes de vigilancia electrónica del FBI. Permite la vigilancia de todas las comunicaciones utilizadas por los terroristas, incluidos los mensajes de correo electrónico, la *internet* (entre ellas *Apple*, *Google*, *Facebook o Microsoft*) a proveer datos a la Agencia Nacional de Seguridad. Tienen su base legal en la USA *Patriot Act* y fue aprobada 45 días después del 11-S casi sin deliberación y en un clima de urgencia[20].

Sin embargo, a pesar de la citada ley, el presidente Bush no parecía convencido de la situación, por lo que la misma fue revisada y actualizada dando como resultado, una segunda edición secreta, la cual especifica:

> Autorización a la Agencia de Seguridad Nacional para espiar a los ciudadanos estadounidenses y extranjeros en los Estados Unidos. La ley mencionaba que sólo se podía espiar a aquellos sospechosos de pertenecer o tener nexos con una organización terrorista. El objetivo del programa era monitorear rápidamente las llamadas telefónicas y otras comunicaciones de personas en los Estados Unidos que se cree tienen contacto con los presuntos colaboradores de Al Qaeda y otros grupos terroristas en el extranjero[21].

Por lo tanto, actualmente, el gobierno estadounidense reconoce que han realizado varias actualizaciones a esta ley, sin embargo, en la página oficial de su gobierno se menciona lo siguiente:

> Aunque ha sido impugnada por grupos de los derechos civiles en los Estados Unidos por vulnerar los derechos de privacidad y confidencialidad de la información,

---

[20] Laia Tarragona. *El Estado de derecho frente al estado espía*. CIDOB. Investigadora CIDOB. 2013. Opinión CIDOB. [En línea]. http://www.cidob.org/es/publicaciones/opinion/seguridad_y_politica_mundial/el_estado_de_derecho_frente_al_estado_espia. [Página consultada el 29/ XI/ 2018].

[21] Dan Eggen. Washington Post. *Bush Authorized Domestic Spying*. [En línea]. 16 de diciembre 2005. https://www.washingtonpost.com/archive/politics/2005/12/16/bush-authorized-domestic-spying/6c4d8e50-8bf9-4164-bdc3-100bb7bcfa71/. [Página consultada el 29/ XI/ 2018].

> sigue vigente y con más fuerza. Es una ley extraterritorial, abarca jurisdicción internacional y se apoya en los tratados internacionales y convenios bilaterales. En *U.S. InterAmerican Affairs*, hemos extractado en este caso el título III para su publicación, referente a la financiación del terrorismo, a través del lavado de dinero y activos y actividades ilegales con respecto a Bancos, Entidades Financieras, Empresas y Corporaciones Multinacionales, personas jurídicas e individuos que sean incluidos en las listas OFAC. Es una Ley de aplicación obligada para hacer negocios con los Estados Unidos y los países miembros de las Naciones Unidas, en combinación con las Leyes *U.S. Sarbanes Oxley, U.S. Victory* y las normas y regulaciones como Control Interno C.O.S.O. Nuevo marco del Gobierno Corporativo" y el Acuerdo Basilea II [22].

De esta manera es como el gobierno estadounidense actualizó la citada ley en el año 2006 y en el 2011 durante la presidencia de Barack Obama.

Por otra parte, considerando que Estados Unidos ha utilizado mano dura contra la sociedad utilizando la vigilancia a su favor, también ha tenido que recurrir a otros mecanismos para lograrlo, tal como el Sistema de *Internet* del Ejército estadounidense *(SIPRNET*) por sus siglas en inglés, ante lo cual se puede señalar.

> El SIPRNET se creó después del ataque del 11S, cuando se detectaron unos fallos de coordinación entre los servicios de inteligencia que recomendaron la necesidad de un modelo de comunicación que permitiera a los diferentes responsables de la seguridad compartir datos extraídos por el Departamento de Estado[23].

Interesante es mencionar que, de acuerdo con *The Guardian*, este es un protocolo de *internet* secreto, diseñado para atacar a grandes burocracias y mantener el control de la información confidencial. Actualmente es un sistema de control militar mundial dirigido por Washington y que muchas embajadas han contratado y utilizado para mantener un canal de comunicación entre posibles ataques y la Agencia de Inteligencia; es decir, para sentirse un poco más seguros a pesar de la vigilancia 24/7 que conlleva.

Así, para concluir este apartado, se puede decir que, del análisis hasta aquí efectuado, surge un tercer término llamado Sociedades de Control (SC) mismo que juega un papel fundamental en el sistema y principalmente en el tema de la privacidad social y vigilancia.

---

[22] Ley Patriótica de los Estados Unidos. *United States Interametican Community Affairs*. [En línea]. http://interamerican-usa.com/articulos/Leyes/US-Patriot%20Act.htm. [Página consultada el 15/ XII/ 2018].

[23] El Universal Internacional. *Estados Unidos invierte $53.000 millones en espionaje*. 31 de agosto de 2013. [En línea]. http://www.eluniversal.com/internacional/130831/EE.UU.invierte-53000-millones-en-espionaje. [Página consultada el 29/ XI/ 2018].

Pero ¿qué entender por las Sociedades de Control? Sin duda, las SC tienen un importante papel en el tema de la vigilancia, misma que actualmente es parte de un fenómeno natural problematizado, pero que hoy está normalizado por los individuos, es decir, el modelo panóptico y/o súper panóptico, el cual ejemplifica que en la vida cotidiana los individuos se acostumbran a estar dentro de una oficina, escuela, hogar sin verle mayor complicación asegurando que perciben mayor seguridad si se encuentran en ellas.

Por tanto, entiéndase que las SC son perfectas máquinas de miedo, se desarrollan mediante dispositivos hechos para enfrentarlos en cualquier lugar con inseguridad, es decir, cualquier motivo de nula seguridad para el individuo conduce a una transformación de disciplina[24].

Así, parece irónico que la vigilancia parezca un mal necesario para la sociedad, una paranoia de sentirse *con* seguridad sin notar que hoy en día se vive, bajo una especie *de* control en el que el saber que no se debe ni se puede quebrantar la ley es la mejor forma de espionaje. Sin duda alguna, dígase que, tras el ataque del 11S no se han dejado de implementar proyectos para aumentar la vigilancia y mantener una relación privacidad-público con una línea muy delgada en toda la comunidad internacional.

Dado lo anterior, usemos el pensamiento de Manuel Castells, el cual considera que, gracias a la tecnología, el mundo se ha vuelto más pequeño por lo que la única condición para participar en una sociedad de control es ser capaz de compartir protocolos y códigos de comunicación. Ante esto, para el citado autor: “El Estado nos vigila y el Capital nos vende, o sea, vende nuestra vida transformada en datos”[25].

Bajo esta interesante reflexión, lo que Castells quiere indicar es que, las grandes cabezas de inteligencia junto con los gobiernos tratan de cuidar al ciudadano mediante un sistema muy bien estructurado de vigilancia, mismo que, después vende a grandes empresas y al mismo Estado con la información cautelosa y legalmente guardada. Quien sustenta este trabajo cuestiona ¿será esta la nueva vigilancia característica del Siglo XXI?

1.3. La vigilancia en el Siglo XXI

Reconociendo que la vigilancia ha traído a la historia del S. XXI sucesos interesantes que requieren atención, no cabe duda de que, el derecho a la privacidad se ha vuelto intangible,

[24] Manuel Castells. *Vivir en un estado de vigilancia permanente*. https://ssociologos.com/2015/03/12/vivir-en-estado-de-vigilancia-permanente-manuel-castells/. [Página consultada el 08/ I/ 2019].
[25] *Op. Cit.*

pues restringe hasta cierto punto la libertad de los individuos. Al respecto Glenn Greenwald considera que: “Si nunca puedes evitar los ojos vigilantes de una autoridad suprema, la única alternativa es seguir los dictados impuestos por dicha autoridad” [26].

También, para el citado investigador, “la privación de privacidad, mucho más efectiva que una fuerza policial, eliminará toda tentación de infringir las normas” pues “una sociedad en la que todo el mundo se sabe observado por el estado, donde desaparece efectivamente el ámbito privado es una sociedad en la que estos atributos se pierden, tanto en nivel social como individual” [27] .

Las anteriores reflexiones invitan a considerar que, la política exterior estadounidense tiene huellas significativas en su diplomacia gracias a la guerra y durante mucho tiempo ha ostentado el poder gracias a ello. Por tanto, el espionaje ha contribuido de manera significativa a una evolución, pues permite estar a la vanguardia en todos los ámbitos informativos, además que ha propiciado que durante los últimos 30 años se puedan mantener transmisores y cámaras de todo tamaño que con ayuda de satélites hace que nada pase desapercibido de su control.

Dado lo anterior, se sabe que los EE. UU. pueden medir todo al alcance del ser humano, ya sea mensajes de texto, correos electrónicos, llamadas de teléfono y celular y/o fax. De esta forma, la red es tan avanzada que el espionaje se usa en los ámbitos económicos, industriales y demás atacando la privacidad de cualquier modo, al punto que los individuos pierden la capacidad y el derecho de reclamar la misma, ante lo cual Rodríguez señala.

> No es necesaria la ciencia ficción para concebir un mecanismo de control que señale a cada instante la posición de un elemento en un lugar abierto, animal en una reserva, hombre en una empresa (collar electrónico). Félix Guattari imaginaba una ciudad en la que cada uno podía salir de su departamento, su calle, su barrio, gracias a su tarjeta electrónica (individual) que abría tal o cual barrera; pero también la tarjeta podía no ser aceptada tal día, o entre determinadas horas: lo que importa no es la barrera sino el ordenador que señala la posición de cada uno, licita o ilícita, y opera una modulación universal[28].

---

[26] Glenn Greenwald. *Snowden. Sin un lugar donde esconderse*. Metropolitan Books, 2014, Nueva York, 217 pp.

[27] *Ibidem.*

[28] Pablo Esteban Rodríguez. *¿Qué son las sociedades de control*? [En línea]. http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf. [Página consultada el 08/ I/ 2018].

En síntesis, “la vigilancia y espionaje queda definido por la finalidad, aplicación práctica y uso que de lo obtenido se haga para sustentar fines muy dispares. No sólo es, por tanto, una actividad ilícita en sí misma, sino profundamente peligrosa en virtud de la finalidad para la que se emplee la información obtenida”[29].

Opinando acerca de la vigilancia, Navarro señala que la misma canciller alemana Angela Merkel ha expresado que “espiar a los amigos es totalmente inaceptable”[30]

Muchos son los testimonios y acusaciones que en estos años se han hecho unos países a otros sobre vigilancia y espionaje. Un sonado caso fue cuando en mayo de 2014 Estados Unidos acusó directamente a China de llevar a cabo operaciones de espionaje económico. Acto seguido, Pekín exigió la retirada inmediata de la denuncia, realizó una serie de consultas al embajador de Estados Unidos lo que trajo como resultado que se deterioraran las relaciones entre ambos países. El caso se destapó cuando cinco militares pertenecientes a la potente unidad 61398 del Ejército de Liberación Popular chino fueron acusados de espionaje y de haberse infiltrado en las redes de información y comunicación de varias empresas y sindicatos estadounidenses para, a partir de ahí, comenzar a extraer informaciones confidenciales.

Pero el estar señalando casos no es lo más importante, sino como lo opina el periodista Glenn Greenwald, lo atractivo es la trascendencia del debate global sobre lo ocurrido, pues:

> Por primera vez, hay un debate público mundial sobre el valor de la privacidad y la intimidad en *Internet*. Además, algunos países están poniendo en marcha reformas para limitar la vigilancia de los ciudadanos y para evitar que EE UU domine la Red. Hay empresas de telecomunicaciones norteamericanas que tienen mucho miedo de los efectos del espionaje en sus propias instalaciones, porque la gente no va a querer utilizar ni Facebook ni Google ni nada si piensa que los datos se pueden captar. El cambio más importante de todos es que la gente se ha dado cuenta de hasta qué punto se ha puesto en peligro su intimidad y su privacidad y ahora muchas personas están empezando a usar sistemas de encriptación para proteger sus comunicaciones y evitar así que los vigilen[31].

Por tanto, debe entenderse que, ser tecnológicamente dependiente suele tener consecuencias negativas ya que, si nos encontramos con un país que no cuenta con las

[29] Diego Navarro Bonilla. [En línea]. https://es.scribd.com/document/433998032/Us-PDF-170933. [Página consultada el 08/ I/ 2018].
[30] Navarro, *Op. cit. p. 31*
[31] *Ibid*, *p. 33*

capacidades técnicas para desarrollar programas, puede tener desventaja estratégica ante otros países, lo que podría representar desigualdades, pero, el asunto no es determinar si se espía o no, pues lo trascendente es si se puede hacer con la tecnología disponible por un país. Y para resaltar el importante papel de los datos, Navarro explica:

> En el contexto que contrapone la información al conocimiento, una nueva dicotomía ha aparecido: la de los riesgos del *Big Data* frente a la comprensión y al análisis (*big narrative*). Hace una década que se viene manejando una frase como un mantra: el reto es el análisis, no la obtención. El objetivo no es el análisis, sino la predicción: del *Big Data* al *big foreknowledge*. El destino es la prospectiva o los estudios de futuro. Si el objetivo era controlar, ahora es predecir conductas o acciones a corto/medio/largo plazo. Y ahí los datos son, como tantas veces se ha repetido, el nuevo oro[32].

1.4. Adelantos de la vigilancia internacional

Como antes se mencionaba, la vigilancia se generaliza a través de las redes sociales, el ejercicio de exhibirse públicamente permite a los operadores de seguridad y consumo levantar los perfiles, es decir tienen la capacidad de mantener una base de datos segmentada. La información necesaria para estos segmentos también está proporcionada por los teléfonos celulares personales, la modernidad líquida ha convertido a todo mundo en sospechoso sin control de su seguridad personal.

Ante esto, Pilar Calveiro refiere a la vigilancia como las formas de violencia, mismas que define como: Las formas específicas que asume el uso de la fuerza institucional (…) formas de organización de poder político[33].

Calveiro resalta el totalitarismo, mismo que se encuentra vinculado al fascismo, nazismo y por último al estalinismo. Estos se concentran en indicadores de diferencias ideológicas. Marca como una de las diferencias al *globalitarismo y biopoder* de Foucault como medios de actualización del totalitarismo en el marco neoliberal del Siglo XX; en este se engloban las modalidades de violencia estatal, matices totalitarios, sociedad contemporánea y guerras antiterroristas. En todas ellas se pueden observar puntos de conexión de formas represivas haciéndose una red corporativa transnacional con la

[32] *Ibid, p. 39*
[33] Pilar Calveiro. *Violencias de Estado. La Guerra antiterrorista y la Guerra contra el crimen como medios de control globa*l. [En línea]. file:///C:/Users/Laura%20Gonzalez/Downloads/37-71-1-SM.pdf. [Página consultada el 08/ I/ 2018].

capacidad de articulación entre los territorios que, con ayuda de los gobiernos estatales, pueden acceder a flujos económicos, culturales, sociales y políticos.

Así, la red que se define como global se mueve de un lado a otro dejando en cada sitio flujos de poder capaces de realizar operaciones unidireccionalmente. Como tal, se podría decir que, el mundo se encuentra en modo bipolar con tendencias a violencias globales. El enemigo externo como le llama Calveiro al terrorismo, está asociado con una lista de acciones determinadas, como, por ejemplo, la violencia replicada ya sea en procesos sociales, políticos o actos normativos de organismos gubernamentales e internacionales.

Opinando al respecto otro autor como Fernández explica que:

> "La sociedad también se identifica por ser una red, que se caracteriza por la transformación sociotécnica del espacio, del tiempo, la cultura y el Estado. Es una sociedad capitalista, pues, en un principio, la evolución hacía las formas de gestión y producción en red no implica la desaparición del capitalismo, sino su renovación hacía un nuevo tipo de capitalismo global".[34]

Se puede decir que, este es el punto donde se encuentra el riesgo de constitución de un instrumento de control político sobre cualquier tipo de protesta social, pues sin duda, "el terrorismo consiste en el uso de violencia masiva e indiscriminada contra una sociedad o un grupo de ella (…) usando el terror como mecanismo de control e inmovilizador social"[35].

Así, algunas de las cualidades de este inmovilizador son: redes globales antiterroristas, terroristas con reivindicación, movimientos armados de resistencia y como un punto importante a agregar, las operaciones militares, políticas y económicas que se dieron a partir del 11S. Además, un lazo cercano a estos inmovilizadores es la tortura, ante la cual, EE. UU. es uno de los grandes maestros de la misma. Considérese que, han existido leyes por tratar de eliminarla sin éxito por lo que se ha llegado a leyes para flexibilizar la tortura a partir de su redefinición y/o aceptación en instituciones de seguridad.

También, se puede incluir en todas estas cualidades las que están alimentadas por tecnología de información, pues en la actualidad, las estructuras más eficientes por su dinamismo, flexibilidad y lógica común de la sociedad; son capaces de conectarse alrededor de todo el mundo desde un punto y así tener la visibilidad de las distintas plataformas de

---

[34]Miguel Héctor Fernández-Carrión. *Control social en la sociedad de red*. Nóesis. Revista de Ciencias Sociales y Humanidades. México. 2007. [En línea]. https://dialnet.unirioja.es/servlet/articulo?codigo=2265397. [Página consultada el14/XII/ 2018]. Pp. 88.

[35] *Ibídem.*

comunicación. Estas instituciones son principalmente las cárceles, mismas que tienen una conexión entre la represión legal y la ilegal.

Ejemplificándolo quedaría: la legal son las detenciones reconocidas (caso de migrantes) y la ilegal son las prácticas de tortura dentro de las instalaciones para fines de obtención de información y desaparición forzada. Es entonces cuando se puede dar cabida a lo que se llama *doctrina del shock* donde se explica como el capitalismo utiliza y emplea violencia y terrorismo contra la sociedad actual, aprovechando las crisis para realizar todo tipo de torturas como medidas económicas y políticas.

Así, para Calveiro, a final de cuentas la relación entre las sociedades de control es la vigilancia y la vigilancia para Foucault "es un fenómeno a la vez individualizador y masificante, un aparato institucional dedicado a lograr el autodominio del sujeto y su sujeción, mientras se recaban los datos posibles que puedan hacerlo entrar en otro régimen de visibilidad. Este régimen es el biopolítico, ante lo cual Rodríguez considera que: Muchas veces se desconoce que el vínculo entre la anatomopolítica (disciplina) y la biopolítica (población) se halla en este carácter bifronte de la vigilancia"[36].

Por tanto, no cabe duda de que la relación entre la vigilancia y el encierro se vinculan por la necesidad de no ocultar sobre la conciencia del ya vigilado. Así, las normalizaciones de estos instrumentos utilizados por el Estado dan apertura a todas las actividades realizadas por un individuo. Ante ello, Foucault decía que este tipo de disciplina sufría la tendencia de caer en una producción, es decir, revisar todo tipo de información y al final acumularla como objetos que pueden ser utilizados en cualquier momento y que pueden tener como primer esquema el miedo, el temor a la violencia, la discriminación, exclusión y pobreza, dando empoderamiento a las sociedades de control.

1.5. Impacto social

Se considera relevante señalar lo que debe entenderse por *impacto social*. En este orden de ideas Liberta Bonilla explica que, la utilización del término impacto se ha ampliado y este ha sido objeto de múltiples definiciones en la literatura referida a los problemas sociales, entre las que se encuentran las siguientes:

- "El impacto se refiere a los efectos que la intervención planteada tiene sobre la comunidad en general.

[36] Rodríguez, *Op. cit.*

- El impacto puede verse como un cambio en el resultado de un proceso (producto).
- El impacto social se refiere al cambio efectuado en la sociedad debido al producto de las investigaciones.
- El impacto de un proyecto o programa social es la magnitud cuantitativa del cambio en el problema de la población objetivo como resultado de la entrega de productos (bienes o servicios).
- Los impactos son los logros derivados del desarrollo de un proyecto y que pueden observarse a largo plazo (después de año y medio)"[37].

Por tanto, bajo esta línea de pensamiento, este trabajo se dividirá en diferentes subcapítulos destinados a explicar cada una de las consideraciones hechas para la ejemplificación de la afectación a la seguridad social. Es complejo acotarlo ya que se ha encontrado el registro de muchos casos de afectación en la actualidad.

1.5.1. La afectación a los Derechos Humanos

En nuestro país, la misma Comisión Nacional de Derechos Humanos (CNDH) ha considerado que, si bien la intervención de las comunicaciones no está prohibida, la Constitución Política de los Estados Unidos Mexicanos establece que la única vía legal para hacerlo es mediante una orden judicial, por lo que contravenir ese mandato con el objetivo de conocer la vida personal y profesional, entorpecer o afectar la labor de periodistas y personas defensoras de derechos humanos, constituye una violación y una afectación a los mismos derechos humanos, delito que debe ser investigado y sancionado. En este sentido, "La CNDH ha señalado que "condena toda conducta que busque afectar la privacidad de las personas, pues afecta su intimidad y sus derechos humanos y estará atento a la investigación de las autoridades de procuración de justicia"[38].

El mismo titular de la CNDH, Luis Raúl González Pérez ha mencionado:

> Toda grabación fuera de los preceptos del artículo 16 constitucional es totalmente ilegal. La posición es condenar que nadie está autorizado para incidir en nuestra privacidad al margen de la ley. Vivimos en un estado democrático de derecho. Cuando hay escuchas que no cumplieron las formalidades legales, quien lo realice incurre en responsabilidades que tienen

[37] Enrique Liberta Bonilla. "Impacto, impacto social y evaluación del impacto. Acimed". [En línea]. http://scielo.sld.cu/pdf/aci/v15n3/aci08307.pdf [Página consultada el 22/V/ 2019].
[38]CNDH. "Comunicado de Prensa DGC/203/17". [En línea]. http://www.cndh.org.mx/sites/all/doc/Comunicados/2017/Com_2017_203.pdf. [Página consultada el 29/V/2019].

> que ser investigadas porque constituyen delitos que hay que investigar. Si las autoridades no cumplieran con las formalidades de ley, estarían violentando las normas[39].

También, actores políticos como Marko Cortés -presidente del Comité Ejecutivo Nacional del PAN- señaló que:

> El espionaje político es un abuso desde se le vea. Es el uso de instrumentos del Estadio contra los ciudadanos. Es una violación a los Derechos Humanos que daña la democracia, y que atenta contra aquello que en primer lugar debe proveer el Estado a la gente: seguridad. El espionaje coloca al vigilado en una situación de vulnerabilidad, en el que asuntos privados, familiares, financieros, laborales, de salud, pueden ser usados en su contra, ilegal y ventajosamente, desde los sótanos gubernamentales[40].

Como es lógico suponer, muchas fueron las opiniones vertidas cuando se descubrió el espionaje a periodistas mexicanos, como la de Luis Fernando García, director de la Red en Defensa de los Derechos Digitales (R3D) el cual afirmó en su momento que "el hecho de que el gobierno esté usando vigilancia de alta tecnología en contra de defensores de derechos humanos y periodistas que exponen la corrupción, en lugar de contra los responsables de estos abusos, dice mucho de para quién trabaja el gobierno"[41].

1.5.2. El trabajo de las Organizaciones No Gubernamentales

En este caso, cabe señalar a algunos organismos que colaboraron en la creación de los denominados Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (comentados en el siguiente punto), como, por ejemplo:

- *Privacy International* (responsable de la denuncia del gobierno británico por la operación del programa Tempora).
- *Electronic Frontier Foundation* (pionera en Estados Unidos en la defensa de los derechos civiles vinculados al mundo digital.
- *Access* (organización dedicada a la promoción de los derechos digitales en todo el mundo).
- Asociación Civil por la Libertad y la Justicia (Argentina)

---

[39] Proceso. "Espionaje viola los derechos humanos, hay que investigarlo: CNDH". [En línea]. https://www.proceso.com.mx/410887/espionaje-viola-los-derechos-humanos-cndh. [Página consultada el 29/V/2019].

[40] El Universal. "Espionaje: grave violación a los derechos humanos". [En línea]. http://www.eluniversal.com.mx/entradadeopinion/articulo/markocortes/nacion/2017/07/11/espionaje-grave-violacion-los-derechos. [Página consultada el 29/V/2019].

[41] The New York Times. "Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México". [En línea]. https://www.nytimes.com/es/2017/06/19/mexico-*Pegasus*-nso-group-espionaje/. [Página consultada el 30/V/2019].

- Fundación Karisma (Colombia)[42].

La ya citada R3D es "una organización mexicana dedicada a la defensa de los derechos humanos en el entorno digital, la cual utiliza diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México, particularmente, la libertad de expresión, la privacidad, el acceso al conocimiento y la cultura libre".[43]

En cuanto al tema de privacidad, se sabe que:

> R3D inició su labor en la defensa de la privacidad en México a raíz de la discusión del Código Nacional de Procedimientos Penales (CNPP) a finales de 2013, que contemplaba la intervención de comunicaciones privadas, incluyendo la geolocalización y la recolección y acceso a metadatos. A partir de dicha labor de incidencia legislativa, la organización trabaja en diversas líneas estratégicas relacionadas a la privacidad en el entorno digital de las y los mexicanos. R3D mantiene también una investigación y análisis permanente a las capacidades tecnológicas para la intervención de comunicaciones y la invasión a la privacidad que poseen autoridades federales, gobiernos locales y distintas dependencias en México[44].

En 2013 en un contexto de represión del Estado y de manifestaciones públicas surge la Red #RompeElMiedo, para responder a la necesidad de proteger a quienes estaban arriesgando su integridad y libertad para documentar violaciones a los derechos humanos y arbitrariedades perpetradas principalmente por las autoridades. En sus inicios, la Red se formó por iniciativa de un grupo reducido de medios libres y colectivos, incluso con voluntarios e integrantes del todavía existente movimiento #YoSoy132, que ofrecían su tiempo para monitorear a quienes acudían a las protestas.

> En la actualidad, la Red #RompeElMiedo tiene presencia en los 32 estados del país, está compuesta por más de 800 periodistas y ha logrado articularse y coordinar esfuerzos con una docena de organizaciones locales de derechos humanos y periodistas[45].

Cabe señalar que, el objetivo principal de esta ONG es empoderar a periodistas y comunicadores en temas de seguridad integral (física, digital y psicosocial) para que puedan ser más resilientes antes los riesgos y amenazas que enfrentan.

---

[42] Diario Turing. Galldon Clavell Gemma. "Espionaje y derechos humanos: los límites a la intromisión de la intimidad". [En línea]. https://www.eldiario.es/turing/Espionaje-derechos-humanos_0_159934512.html. [Página consultada el 02/VI/2019].
[43] Red de Defensa de los Derechos Digitales. [En línea]. https://r3d.mx/privacidad/. [Página consultada el 02/VI/2019].
[44] *Op. Cit*
[45] Red Rompe el Miedo. "Elecciones 2018". [En línea]. https://r3d.mx/wp-content/uploads/RRM-2018.pdf. [Página consultada el 03/VI/2019].

Parte también importante en el juego de la privacidad y el espionaje lo son las empresas de telecomunicaciones en México y, en este sentido, en un documento denominado ¿Quién no defiende tus datos?, R3D llega a interesantes y valiosas conclusiones, no sin antes señalar que, la Ley Federal de Telecomunicaciones y Radiodifusión contempla en sus artículos 189 y 190 diversas obligaciones de colaboración en materia de seguridad y justicia por parte de los concesionarios y autorizados de telecomunicaciones. Las conclusiones a las que llegó R3D son:

- El incumplimiento de los lineamientos en materia de seguridad y justicia por parte de las empresas de telecomunicaciones -al no presentar informes o no cumplir al entregar información incompleta o incierta- junto con la omisión por parte del Instituto Federal de Telecomunicaciones de publicar los informes recibidos y de solicitar los informes correspondientes a autoridades facultadas para ejercer vigilancia, para el periodo 2016-2017, representan importantes obstáculos para la transparencia en materia del ejercicio de vigilancia estatal.
- La información revelada por los informes semestrales para el periodo 20162017 sugiere violaciones sistemáticas al derecho a la privacidad y la protección de datos personales por parte de empresas de telecomunicaciones, al otorgar acceso a datos personales de los usuarios a autoridades no facultadas en el ejercicio de la vigilancia.
- Con la derogación de las obligaciones de transparencia, las empresas de telecomunicaciones cuentan aún con menores incentivos para proteger la información de sus usuarios por lo que es posible que la proporción de los casos de abuso aumente o se perpetúe. La modificación de los lineamientos elimina un valioso recurso para inhibir malas prácticas y no permite al IFT cumplir con sus obligaciones de supervisión y sanción relacionadas con la privacidad de las comunicaciones de las y los usuarios.
- Las empresas de telecomunicaciones deben continuar produciendo y publicando informes de transparencia relacionados con la colaboración en materia de seguridad y justicia, independientemente de la ausencia de un requerimiento legal para ello.
- Debe contemplarse la formulación de procesos educativos, en las que participen representantes de gobierno, poder judicial, órganos constitucionales autónomos, expertos de la sociedad civil, academia e industria que permitan a las concesionarias y autorizadas de telecomunicaciones y a otras partes interesadas, conocer las mejores prácticas de debida diligencia y transparencia en la colaboración en materia de seguridad y justicia en aras de mejores procesos para la protección de la privacidad de las y los usuarios de telecomunicaciones[46].

[46] R3D. ¿Quién no defiende tus datos? 2018, [En línea]. https://r3d.mx/wp-content/uploads/R3D-QNDTD_digital.pdf. [Página consultada el 03/VI/2019].

Por tanto, si el espionaje y la vigilancia ya sea de carácter nacional o internacional está cada día más presente, afectando los intereses, derechos humanos y privacidad de las personas, la respuesta más lógica a ello sería que los Estados diseñen y creen leyes, reglamentos y normatividad que proteja a las personas de dicha actividad. Así, enseguida se verificará como algunos países ya cuentan con disposiciones al respecto.

1.6. Legislación creada sobre espionaje y vigilancia internacional

Los siguientes documentos que se mencionan son el resultado de la búsqueda de legislación existente para proteger a las personas del espionaje y la vigilancia.

- **Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.** Los siguientes principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y expertos internacionales en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología. Tabla realizada con información tomada del sitio web de Necessary & Proportionate.

Tabla 2. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

Legalidad. Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación**.**
Objetivo legítimo. Las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición**.**
Necesidad. Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.
Idoneidad. Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.
Proporcionalidad. La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar

la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.
Autoridad judicial competente. Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe: Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones. Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.
Debido proceso. Exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general.
Notificación del usuario. Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización.
Transparencia. Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.
Supervisión pública. Los Estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales.
Integridad de las comunicaciones y sistemas. A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "*hardware*" o "*software*" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado.
Garantías para la cooperación internacional. En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estándar disponible con el mayor nivel de protección para las personas.
Garantías contra el acceso ilegítimo y derecho a recurso efectivo. Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los *whistle blowers* y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información.

Fuente: Necessary & Proportionate. *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. [En línea]. https://necessaryandproportionate.org/es/13-principles/ t. [Página consultada el 05/VI/2019].

- **Ley de Seguridad Nacional (México).** En nuestro país, el 31 de enero de 2005 se publicó en el Diario Oficial de la Federación la Ley de Seguridad Nacional teniendo como objeto, establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la Seguridad Nacional, en sus respectivos ámbitos de competencia; así como, la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea; regular los instrumentos legítimos para fortalecer los controles aplicables a la materia[47].

Cabe señalar que, la Ley de Seguridad Nacional en su capítulo II de las intervenciones de comunicaciones, señala en su articulado lo siguiente:

> Artículo 33.- En los casos de amenaza inminente a los que se refiere el artículo 5 de esta Ley, el Gobierno Mexicano podrá hacer uso de los recursos que legalmente se encuentren a su alcance, incluyendo la información anónima.
>
> Artículo 34.- De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología[48].

- **Ley Especial contra los Delitos Informáticos de la República Bolivariana de Venezuela**.

  Fue firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los cuatro días del mes de septiembre de dos mil uno, teniendo por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley. Consta en total de 31 artículos y en el artículo 11 señala:

[47] Cámara de Diputados del H. Congreso de la Unión. "Ley de Seguridad Nacional". [En línea]. http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf. [Página consultada el 05/VI/2019].
[48] *Op. Cit.*

Artículo 11º Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.[49]

- **Código Penal Español.** En el caso de España, el delito contra la privacidad está tipificado en el artículo 197.1 del CPE que a la letra dice:

  El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses[50].

La siguiente tabla de elaboración propia resume el tratamiento que se ha dado a los delitos informáticos en otras latitudes con información tomada de distintos sitios de *internet* que nos hablan de la legislación en diferentes países sobre los delitos informáticos.

Tabla 3. Tratamiento a los delitos informáticos en otros países.

País/Organismo	Situación
Alemania	Para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos; Estafa informática; Falsificación de datos probatorios; Alteración de datos; Sabotaje y Utilización abusiva de cheques o tarjetas de crédito.
Austria	La Ley de reforma del Código Penal de 22 de diciembre de 1987 contempla el delito de Estafa informática, mismo que sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso

[49] *Gaceta Oficial de la República Bolivariana de Venezuela Ley Especial contra los Delitos Informáticos*. [En línea]. https://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf. [Página consultada el 05/VI/2019].

[50] *"¿Qué leyes viola el espionaje de la NSA y cómo puedes defenderte?".* [En línea]. https://hipertextual.com/2013/10/claves-legales-espionaje-nsa. [Página consultada el 06/VI/2019].

	del procesamiento de datos. Además, contempla sanciones para quienes cometen este hecho utilizando su profesión.
Francia	La Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático contempla como delitos: Acceso fraudulento a un sistema de elaboración de datos; Sabotaje informático; Destrucción de datos; Falsificación de documentos informatizados y Uso de documentos informatizados falsos.
Estados Unidos	Desde 1986 cuenta con el Acta Federal de Abuso Computacional. Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para quienes lo transmiten de manera imprudencial la sanción se encuentra entre una multa y un año de prisión.
La posición de la ONU	Para este organismo, los problemas que rodean a la cooperación internacional en el área de los delitos informáticos son: "falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos; ausencia de acuerdos globales en la definición legal de dichas conductas delictivas; falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos; no armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos; carácter transnacional de muchos delitos cometidos mediante el uso de computadoras y ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional. Por tanto, en septiembre de 2003 entró en vigor la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, principal instrumento internacional en la lucha contra la delincuencia organizada, contemplando las infracciones informáticas.
Convenio de Cibercriminalidad de la Unión Europea	Firmado el 21 de noviembre del 2001 en Budapest, el cual fue impulsado por el Consejo de Europa y otros países como Estados Unidos y Japón. Busca como objetivos fundamentales: Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y Establecer un régimen dinámico y efectivo de cooperación internacional.

Fuente: *Legislación en diferentes países sobre los delitos informáticos* [En línea]. https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm. [Página consultada el 06/VI/2019].

Si bien existen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y Convenio de Cibercriminalidad de la Unión Europea su alcance es ético, siendo deseable y necesario que se conforme leyes y reglamentos de carácter internacional, pues de lo contrario el nicho de mercado que tienen ante sí los grupos de la delincuencia organizada (estatal o no) es muy amplio.

Por ejemplo, tómese en cuenta que, por lo que corresponde a nuestro país, el gobierno mexicano espió a periodistas y defensores de derechos humanos, siendo los casos más conocidos los de los periodistas Carlos Loret de Mola, Carmen Aristegui, el

Centro de Derechos Humanos Miguel Agustín Pro-Juárez, A.C., el Instituto Mexicano para la Competitividad, A.C. y mexicanos contra la Corrupción y la Impunidad, de los cuales se hablará en el segundo capítulo.

1.7. Retos por vencer

Sin duda alguna, parecería interminable enlistar todos los urgentes compromisos que demandan los retos que enfrenta la sociedad en cuanto a espionaje y vigilancia, pero, como explica Navarro, para desarrollar un verdadero control de la actividad de inteligencia se debe contar con una voluntad política y que también se cuenten con medios materiales, es decir, que el órgano de control disponga de amplias facultades y que su actuación quede amparada por un amplio consenso social sobre el interés de la actividad de inteligencia, pero también de su sometimiento estricto a la ley.

Por su parte, en opinión de Barrera e Ibáñez: "América Latina y el Caribe tienen el reto de garantizar su propia seguridad, sin la tutela de las grandes potencias, pues los medios y vías a través de los cuales las potencias conciben la seguridad propia son generalmente lesivos y atentatorios a las de terceros Estados, salvo que estos acaten las onerosas y degradantes condiciones que le son impuestas"[51].

Ahora, al referirse a los servicios de inteligencia y la estrategia de seguridad nacional, Leonardo Curzio señala:

> Un elemento clave para articular los principios generales del Estado con la política y la estrategia de seguridad nacional es el funcionamiento de los servicios de inteligencia…A fin de reducir las asimetrías que la situación actual provoca, sería necesario que México alcanzara dos objetivos: proyectar prestigio como país en esta materia y desarrollar una red de información suficientemente sólida, basada en la realidad de la región, sin que esto se convierta en una amenaza ni en una violación de la soberanía de otros países… Para consolidar la democracia en México es primordial que uno de sus pilares más sólidos sean los servicios de inteligencia -profesionales y con vocación democrática- sobre todo en estos momentos, en el que algunos cuerpos de seguridad (policías) parecerían estar conspirando contra la paz pública y la tranquilidad del país… En lo tocante a la seguridad nacional, México enfrenta un desafío conceptual de primer orden: definir

[51] Palacios Barrera, H; Díaz Ibáñez, E. *La seguridad en el Caribe. retos, desafíos y amenazas para la integración* Ciencia en su PC, núm. 3, 2008Centro de Información y Gestión Tecnológica de Santiago de Cuba Santiago de Cuba, Cuba, pp. 96-107.

> con claridad su proyecto como país para los próximos años, de manera que de esa formulación general se desprendan los objetivos y los intereses nacionales[52].

Para despedir este capítulo, usemos el pensamiento de Navarro, el cual cita:

> Snowden ha marcado un punto de inflexión. No ha sido el único, porque ha habido un número importante de casos de filtraciones durante todo el Siglo XX. Lo que lo hace sobresaliente es la magnitud. Querer espiar a todos todo el tiempo y en todo lugar sólo muestra una realidad bastante desilusionante: la incapacidad por discriminar lo que realmente importa. Cuando todo es espionaje, nada es inteligencia[53].

Por su parte, Ricoy Casas, al analizar algunos ejemplos de espionaje y vulneración de la protección de datos a escala mundial, considera que:

> Las instancias supranacionales y mundiales asoman por la fuerza de los hechos en el horizonte político del planeta, propiciando nuevas formas y estructuras políticas e institucionales, nuevas formas e imágenes de gobernabilidad, más amplias, integradoras y globalizadas. Asimismo, se confirma la necesidad de esta tendencia de establecer una estrecha interconexión entre lo local, lo nacional y lo global, produciéndose al mismo tiempo un gradual desbordamiento y perforación del sistema de soberanía estatal. Ámbitos como la protección de datos o el espionaje a nivel internacional avalan esta tesis e imponen un cambio de paradigma jurídico, Por tanto, el pensamiento anterior debe conducir a reconocer que, y político para hacer frente a esta nueva realidad global[54].

Por tanto, el pensamiento anterior debe conducir a entender que, lo primero, fueron las cámaras de seguridad en bancos y cajeros, más tarde, en lugares públicos, y ahora una intromisión general, dando lugar a que la privacidad que existía sea violentada en la vida de las personas para que puedan ser controladas -con la excusa de la seguridad- surgen algunas preguntas: ¿cuál es el límite? ¿hasta dónde está dispuesta la sociedad a ceder a cambio de la ilusión de seguridad?

A lo largo de este capítulo se destacaron los primeros antecedentes de la actividad del espionaje, así como el entorno de este, señalando los rasgos de la vigilancia en el Siglo XXI y los adelantos que se tienen. Posteriormente, se analizó el impacto social de esta actividad con relación a los Derechos Humanos y el trabajo de las Organizaciones No

---

[52] Curzio L. *La seguridad nacional en México*. [En línea]. http://www.cisan.unam.mx/pdf/lc02_04.pdf. [Página consultada el 21/VI/2019].

[53] Diego Navarro Bonilla. *Espionaje, seguridad nacional y Relaciones Internacionales.* [En línea]. https://web-argitalpena.adm.ehu.es/pdf/USPDF170933.pdf. [Página consultada el 21/VI/2019].

[54] Ricoy Casas, R.M. *Algunos ejemplos de espionaje y vulneración de la protección de datos a escala mundial*. Revista de la Escuela Jacobea de Posgrado, Nº 14, junio 2018, pp.51.

Gubernamentales. Para culminar el capítulo, se mencionó alguna legislación sobre espionaje y vigilancia internacional, culminando por reconocer los retos que se tienen ante sí en este campo. Así, es probable que lo citado conduzca a las más inquietantes interrogantes, sin embargo, quien sustenta este trabajo, considera que ello debe convertirse en un punto de partida hacia el permanente análisis del tema.

El siguiente capítulo está dedicado a estudiar el entorno y los diversos mecanismos de vigilancia, exponiendo los casos más relevantes de sobre espionaje internacional y también, en nuestro país.

2. EL ENTORNO Y LOS DISPOSITIVOS DE VIGILANCIA

> Un mini dron DJI Phantom -un helicóptero de cuatro hélices y un kilogramo de peso- traspasó las rejas de la Casa Blanca y tras estrellarse con un árbol, cayó finalmente en el jardín sur del inmueble. El mini dron entró debido al error de un aficionado que lo operaba en las cercanías sin ser detectado por los radares sensibles a objetos más grandes, como misiles o aviones. El accidente no tuvo mayores consecuencias, pero llevó a algunos críticos a preguntarse ¿qué habría pasado si el aparato que entró a la residencia del presidente Barack Obama hubiera llevado explosivos o armas químicas?
>
> Guillermo Cárdenas Guzmán
> Colaborador del Cinvestav.

Uno de los mecanismos más importantes para la vigilancia internacional es el espionaje, sin embargo, también el control social representa un importante papel para los procedimientos de disciplina de la sociedad en los espacios. Podemos hablar del momento en el que la privacidad se vuelve mercancía para las empresas privadas y es justo lo que nos mueve a revisar en este capítulo, la vigilancia a un nivel sistémico, la vigilancia como elemento fundamental no solo para el mantenimiento de ciertas relaciones de poder sino para el funcionamiento del sistema capitalista generando ganancias a partir del rompimiento de la privacidad.

Según la autora Shoshana Zuboff las formas de privacidad actualmente se convierten directamente en forma de retribución y acumulación de ganancia, en sus palabras,

> El capitalismo de la vigilancia reclama unilateralmente para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento. Aunque algunos de dichos datos se utilizan para mejorar productos o servicios, el resto es considerado como un excedente conductual privativo («propiedad») de las propias empresas capitalistas de la vigilancia y se usa como insumo de procesos avanzados de producción.[55]

El control de una actividad y la disminución de los tiempos de respuesta han provocado que las conductas y actividades estén en constante vigilancia. Este conjunto de lineamientos

[55]Shoshana Zuboff. La era del capitalismo de vigilancia. [En línea]. https://planetadelibroscom.cdnstatics2.com/libros_contenido_extra/45/44333_La_era_del_capitalismo_de_la_vigilancia.pdf. [Página consultada el 21/V/2021].

establecidos por los estados y/o gobiernos marcan un grado de adquisición de conocimientos para el ataque a quienes consideren enemigos.

Gracias a estos conocimientos, con el tiempo se ha ido mejorando los objetos y actividades en torno a la vigilancia, en este capítulo hablaremos de algunas de ellas tales como lo drones, las aplicaciones, la información en la nube, entre otras. Según Foucault, el triunfo de esto se debería "al uso de dispositivos o instrumentos que modifican y encauzan la conducta de los individuos. Estos instrumentos son la inspección jerárquica, la sanción normalizadora y su combinación en el ejercicio del examen" [56].

Si bien, conocemos que en la situación actual y la vigilancia está de cierta manera representada y ejecutada por el poder militar, Foucault nos hace reflexionar sobre los principios tomados de esta formación para después tomar el poder disciplinario sobre la sociedad y en este caso, sobre otros gobiernos; "hay que señalar que los dispositivos disciplinarios, en su proceso de decadencia, no han desaparecido totalmente, conviviendo con las nuevas formas de poder que empiezan a gestarse tras la Segunda Guerra Mundial"[57], las cuales veremos en el siguiente capítulo.

2.1. Historia de los mecanismos y dispositivos de vigilancia y control

Es posible afirmar que, con el desarrollo de un mundo inmenso en *Internet*, la revolución digital avanza día con día, por lo que la búsqueda en las redes permite establecer el perfil propio de cada consumidor, con lo cual, sin darse cuenta, todo usuario pasa a formar parte de los llamados segmentos, ya sea debido a su edad, preferencias, género, gustos, *hobbies* y/o demás particularidades, dando lugar a la vigilancia masiva, la cual se entiende según la organización *Privacy International* de la siguiente manera.

> Es cuando se espía a poblaciones enteras. La vigilancia masiva es la sujeción de una población o componente significativo de un grupo al monitoreo indiscriminado. Implica una interferencia sistemática con el derecho de las personas a la privacidad (…) Cualquier sistema que genere y recopile datos sobre individuos sin intentar limitar el conjunto de datos a personas definidas como objetivos de vigilancia es una forma de vigilancia masiva[58].

[56]La Sociedad de control. Una mirada al S. XXI desde Foucault. [En línea]. https://www.scielo.cl/scielo.php?pid=S0718-43602017000100317&script=sci_abstract. [Página consultada el 21/VI/2020].
[57] *Op. Cit.*
[58] *La NSA, según las revelaciones de Snowden*. [En línea]. http://www.rebelion.org/docs/234497.pdf. [Página consultada el 09/ IX/ 2018].

Con base en estas ideologías, Estados Unidos desarrolló servicios de inteligencia, llamados actualmente Agencias de Seguridad, siendo una de las principales, la *National Security Agency* (NSA) por sus siglas en inglés. Así, al hacer referencia a este organismo, se considera indispensable remontarse a sus antecedentes.

Sin duda alguna, la Primera Guerra Mundial para Estados Unidos fue complicada, sin embargo, no se había considerado establecer un organismo de espionaje, pues fue a partir de la Segunda Guerra que se desarrollaron programas para organizar este tipo de agencias. Entonces, en 1940 Roosevelt comenzó la organización para recolectar información de todo el mundo o de todos los accesos posibles, a pesar de que esta no era de carácter militar, siendo el ejército la parte fundamental para realizar dicha actividad.

> El ejercicio lo continuó Truman cuando en 1946 se creó la *National Intelligence Authority* agencia en la que las estructuras fueron realizadas por el Departamento de Guerra y bajo la supervisión del Estado llegando de esta manera hasta la Guerra Fría[59].
>
> En cuanto a sus orígenes de la NSA, se sabe que:
>
> Se remontan a los primeros años de la Guerra Fría, cuando en 1952 el presidente Harry S. Truman creó una organización de inteligencia criptológica que, integrada en el recién constituido Departamento de Defensa, sustituyera a la efímera Agencia de Seguridad de las Fuerzas Armadas (1949-1952) en materia de monitorización, procesamiento y análisis de comunicaciones telefónicas y electrónicas de terceros países y protección de las redes propias y aliadas. Durante la Guerra Fría, esta agencia llegó a tener casi 80,000 puestos de trabajo y controlar casi todas las comunicaciones electrónicas procedentes del bloque oriental[60].

A partir de ese momento, la NSA desarrolló las actividades de espionaje a nivel Internacional pasando por la Guerra de Vietnam y teniendo su mayor auge después de los atentados del 11 S.

> La historia reciente de la NSA –o al menos la que se conoce– ha estado marcada por sonados escándalos, fracasos o filtraciones, entre los que destacan la escucha de las comunicaciones de personalidades contrarias a la Guerra de Vietnam o promotoras de los derechos civiles en la década de 1960, los incidentes de los buques espía USS

---

[59] *Foreign relations of the United States, 1945–1950, emergence of the Intelligence establishment*. [En línea]. https://history.state.gov/historicaldocuments/frus1945-50Intel/d160. [Página consultada el 13/XII/ 2018].

[60] *La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EE.UU.* [En línea]. https://www.files.ethz.ch/isn/174181/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf. [Página consultada el18/XII/ 2018], pp. 2.

> Liberty en la costa israelí en la Guerra de los Seis Días (1967) y el USS Pueblo en las costas norcoreanas[61].
>
> Parte muy importante es considerar que:
>
> Desde los sucesos del 11 de septiembre de 2001, la comunidad de inteligencia estadounidense –y en especial la NSA– ha tenido que satisfacer una fuerte demanda de información susceptible de emplearse para la seguridad y defensa del país. Para ello, la NSA ha redefinido y optimizado los procesos que regulan sus relaciones con universidades y empresas con el fin de implementar una gestión del cambio ágil, flexible y acorde a sus necesidades operativas, reduciendo así la burocracia interna y mejorando la eficacia[62].

Lo citado invita a considerar que pareciera ser que, el propósito principal de la NSA es querer saberlo todo, pues cuando todo el mundo esté conectado, obtendrán todos los datos necesarios para llegar a conformar el Imperio de la Vigilancia, en un mundo que parecía increíble hace algunos años, actualmente, los individuos tienen su vida registrada en las redes sociales y en todas las bases de datos en línea.

Bajo esta línea de pensamiento, Michael Foucault expresa que “la vigilancia ocupa un lugar primordial en la organización de las sociedades modernas, que son también sociedades disciplinarias en las que el poder trata de ejercer el mayor control social posible mediante complejas técnicas y estrategias de vigilancia”[63].

Cabe señalar que, esta teoría establece la necesidad de vigilar a la sociedad, actividad que se emite ante el control del Estado, ente que espera controlar todo, teniendo como objetivo vigilar a los individuos, los cuales se sentirán cómodos y sin preocupaciones, pero *sin poder salir*. Se dice entonces, que la seguridad total no existe, sin embargo, la vigilancia está por lograr su objetivo en un corto plazo.

Otra idea relevante de Foucault tiene que ver con el llamado Modelo Panóptico, el cual se basa en la idea de una sensación de omnisciencia invisible. Esto significa que, el Individuo X observa todo sin ser visto. Por su parte, el Individuo Y es el que está continuamente vigilado y vive con temor de ser encontrado. En este caso, este individuo hace o realiza faltas, por lo que normalmente se mantiene disciplinado[64].

---

[61] *Ibidem*.
[62] *Ibidem.*
[63] Iván Torres Apablaza. *Inflexiones Foucalteanas sobre la sociedad de control*. Chile. [En línea]. http://www.redalyc.org/pdf/396/39643561011.pdf. [Página consultada el 09/ IX/ 2018].
[64] Ricardo García Jiménez. *El Panoptismo. Nuevas formas de control social*. [En línea]. https://www.eumed.net/rev/cccss/06/rgj2.htm. [Página consultada el18/XII/ 2019].

Se puede decir que, en la actualidad, el sistema panóptico mantiene una relación con su objetivo principal, sin embargo, ha sido modificado y moldeado por las sociedades de control las cuales tienen como único objetivo mantener bajo vigilancia permanente a la sociedad. La situación aquí es que las redes sociales y el *internet* lo permiten de una forma tan sencilla que todo se mantiene bajo la misma vigilancia.

Por tanto, como es sabido, con las tecnologías desarrolladas hasta ahora, se han multiplicado las estrategias de vigilancia y control, pues antes se daba en los aeropuertos, sin embargo, ahora, esta máxima seguridad aparece en cualquier sitio obligando a los usuarios a no parecer sospechoso, ya que todas las técnicas de captación de datos funcionan para la invasión de la vida privada. Google, por ejemplo, tiene referencia exacta de todos los movimientos que la persona realiza desde su computadora o móvil, dando lugar a un gran archivo que se mueve con ayuda de aplicaciones y precisión en la navegación. Al respecto Orwell opina que "el Gran Hermano quién vigila todo debe al mismo tiempo saberlo todo, conocer a cada individuo, saber los riesgos, tener la completa autoridad para poder vigilarnos, evitar las prácticas secretas y utilizar la capa de una democracia para volverse dictadura en favor de desaparecer la privacidad[65].

Así, lo que en un tiempo parecía propio solo de los libros o la ficción, ahora es una realidad, pues la intimidad es algo que se aleja de la realidad, gracias a las sofisticadas redes de vigilancia utilizadas mediante el uso de la tecnología de información.

Una vez revisado este marco teórico, enseguida se mencionan los principales mecanismos de espionaje y vigilancia.

2.2. Mecanismos modernos de espionaje

Dada la vertiginosa evolución de la tecnología, los siguientes aparatos son solamente una parte de los mecanismos más usados en actividades de espionaje y vigilancia,

> "la recuperación discriminada, ponderada y bien refinada de datos se alza entonces no sólo como una obligación ética y legal de ajuste al derecho de protección de la información personal, sino también un indicador de calidad que redunda en la eficiencia y la eficacia de los resultados: no todos los datos valen para hacer inteligencia. Sin olvidar las implicaciones económicas que tiene la masificación de datos: ¿para qué gastar grandes cantidades de dinero público en sistemas automáticos que recuperan todo de todos?"[66] a continuación de describirán algunos motivos para tal actividad.

[65]George Orwell. *1984*. 2017, Ediciones Leyenda. México, pp.221.
[66] Diego Navarro Bonilla. Espionaje, seguridad nacional y Relaciones Internacionales. [En línea]. https://web-argitalpena.adm.ehu.es/pdf/USPDF170933.pdf. [Página consultada el 21/VI/2019].

2.2.1. Drones

Sin duda alguna, el dispositivo estelar de la vigilancia como estrategia de guerra, lo representan los Drones o *Unmanned Aereal Vehicle* (UAV por sus siglas en inglés) naves robóticas o vehículos manejados mediante control remoto que se dieron a conocer masivamente en los años noventa, aunque su primera utilización fue militar y se contextualizó en la Guerra Fría, para su uso en la Guerra de Vietnam, ello, entre 1955 y 1975.

Así, para comprender el proceso de sofisticación devenido del paradigma de espionaje, vigilancia y necesidad de control militar, es necesario, dar cuenta de algunos procesos relevantes y específicos del desarrollo de la tecnología de los Drones o tecnología no tripulada. Esta tiene su origen en las aeronaves o como bien se les llamaba anteriormente, *torpedos aéreos,* sin embargo, se fueron desarrollando hasta las ahora llamadas naves no tripuladas, pues "los aviones no tripulados han existido y se utilizan desde 1911 pero en la década de 1800 fueron utilizados por primera vez en Austria como globos llenos de bombas, después se desarrollaron naves limitadas durante la Primera Guerra Mundial pero fue hasta la Segunda Guerra Mundial que fueron utilizados para suministrar explosivos contra los alemanes".[67]

Considérese que, la mayor demostración de drones fue en 1991 en la llamada Guerra del Golfo cuando Estados Unidos desplegó vehículos aéreos no tripulados. Tómese en cuenta que, los primeros sistemas de dones fueron desarrollados como armamento de largo alcance. Actualmente, se dice que uno de cada tres aviones no está tripulado y para el año 2012 existían 7,494 vehículos no tripulados según datos de la Fuerza Aérea de Estados Unidos.[68]

La intención de una línea del tiempo sobre la historia de los drones comienza con los europeos; los primeros países en implementar tecnología fue Inglaterra, Alemania, Francia, Rusia, Japón y Estados Unidos; los europeos, tuvieron algunas barreras tecnológicas como el no disponer de un motor con suficiente potencia, cosa que a los estadounidenses les favoreció para realizar un vuelo tripulado con un avión propulsado durante la Segunda Guerra Mundial.

---

[67]Space.com. *What is a Drone*. Howell, Elizabeth. [En línea]. http://www.space.com/29544-what-is-a-drone.html. [Página consultada el 09/ II/ 2018].

[68] Drones estadounidenses. Drones más pequeños y con menos capacidades para el futuro cercano. [En línea]. https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Cuarto-Trimestre-2018/Drones-estadounidenses/. [Página consultada el 09/ II/ 2019].

Durante la Primera Guerra Mundial existieron diferentes vehículos no tripulados. Uno de los pioneros fueron los *Misiles Crucero,* y, a pesar de que no contaban con mucha estabilización automática eran de navegación a control remoto. Ya para 1916 se realiza la primera exhibición de este misil y en 1917 una importante empresa llamada *Curtiss Aeroplane and Motor Company* financia el proyecto con lo cual se tuvieron vuelos exitosos aplicados a cargas explosivas con un motor marca Ford con 40 caballos de fuerza[69].

Por su parte, Gran Bretaña también fue precursor de los misiles durante la Primera y Segunda Guerra Mundial, sin embargo, y a pesar de que desarrollaron algunos modelos, fue hasta 1943 que contaban con al menos veinte modelos diferentes utilizados para la guerra.

En cuanto a los Estados Unidos, se sabe que:

> La empresa *Radioplane Company* se dedicaba específicamente a producir aviones no tripulados para uso de artillería. La producción para la Segunda Guerra fue de aproximadamente 9400 OQ-3 que era un modelo de dron con hélice de propulsión. A finales de 1945 la empresa realizó un diseño diferente con más agilidad y menos pesado; la compañía comenzó a experimentar aviones de gran velocidad y alcance para la Fuerza Aérea sin embargo, en 1952 la empresa fue adquirida por *Northrop* y se convirtió en División *Radioplane* de *Northrop* aunque el nombre fue cambiando paulatinamente[70].

Así, *Northrop* siguió operando hasta la década de los 80´s evolucionando en sus naves no tripuladas, tenían blancos más rápidos y con mayor alcance que fueron equipados con cámaras, operaban a grandes altitudes y al regresar la nave a la base de operación podían ser reveladas las fotografías. Entonces, con la llegada de toda esta nueva tecnología, los estadounidenses sacaron la producción de un vehículo llamado *Firebee* el cual parecía un cohete, ya que era lanzado desde tierra tripulado desde un avión o desde el suelo. Este proyecto fue diseñado a principios de los 60´s siendo su principal para la guerra fría y con los años evolucionó a la medida de un helicóptero o un submarino.

Figura 1. Imagen de sistema no tripulado utilizado en la Guerra Fría llamado *Ryan Firebee*.

[69] *The Curtiss Company.* [En línea]. https://www.centennialofflight.net/essay/Aerospace/Curtiss/Aero2.htm [Página consultada el 019/ III/ 2019].

[70] *The radioplane OQ-2 aereal targer drone was the first quantitaive UAV purchase for the Unitad States*. Military Factory. [En línea]. http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=331. [Página consultada el 019/ II/ 2019].

Fuente: *The Aviation Wing*. [En línea]. https://www.theaviationwing.com/ryan-firebee/. [Página consultada el 019/ III/ 2019].

Durante los años 70´s el tema de la Guerra Fría seguía latente y en continua presión por lo que se desarrollaron otros modelos de drones en los que se incluía la seguridad de comunicación. Uno de los que se realizaron se llamó *Lookheed Aquila* proyecto que pretendía llegar con soldados a la tierra y entregar información en tiempo real. Tenía además la capacidad de identificar enemigos, utilizar láser y sobrevivir a aerodefensas[71].

Durante los años 80 se desarrolló un modelo de inteligencia visual sobre el territorio enemigo. La guía era una pre-programación de un autopiloto al tiempo que transportaban un transmisor de video que podía mandar imágenes del tiempo real a un kilometraje considerable. A finales de los 80´s ya contenían infrarrojo y gracias a ello se lograron lanzamientos y recuperaciones con éxito de la misma manera que los ejércitos seguían buscando extender las operaciones y mejorar la precisión y el control de vuelo.

Durante los años 90 en la Guerra de Yugoslavia sería la última ocasión en la que se usarían aviones tripulados, pues el camino de los drones seguía su avance. Durante estos años también detonaron un sinfín de funciones para las que se utilizan los drones tales como supervisión e inspección de infraestructuras, control fronterizo, vigilancia por Cuerpos de Seguridad, supervisión de instalaciones industriales, uso en medios de comunicación, gestión de recursos naturales, estudios ecológicos, seguimiento de especies, para meteorología, atención a personas y entretenimiento.

[71]*Directory of U.S. Military Rockets and Missiles*. [En línea]. http://www.designation-systems.info/dusrm/m-105.html. [Página consultada el 019/ III/ 2019].

Si bien a finales del Siglo XX se presenció un cambio en la dirección del uso de los drones a principios del año 2000 se pudo observar un incremento en el uso militar y en comparación con años anteriores se acumularon muchas más horas de uso de los mismos.

Se construyeron drones con tecnología de defensa, si eran identificados podían atacar inmediatamente al enemigo, además de ser casi indetectable gracias a sensores y capacidad para volar a mayor altura. Actualmente hay organizaciones que proponen la regulación de estas nuevas armas, una de ellas es la NASA que expone un enfoque más científico que bélico y llevar a cabo pruebas de muestreo y análisis de las capas atmosféricas.

> En el año 2001 se utilizó a los drones como arma directa de ataque a partir de la Guerra de Afganistán, aunque el aumento de drones coincide con el gobierno de George Bush y Obama se han incrementado las bajas de civiles en otros países y se ha incrementado el número de escenarios donde se utilizaron. Del 2004-2013 tan sólo en Pakistán los drones han matado a 3,460 personas de los cuales muchos pueden ser calificados como *civiles inocentes*[72].

En su mayoría, el incremento y uso de drones ha estado respaldada e impulsada por Estados Unidos, no sólo en el ámbito militar sino también en el comercial ya que la tendencia robótica en el mercado va en constante crecimiento, pues tener un dron se ha vuelto una tendencia. Como se menciona en el inicio de este capítulo, si bien se puede observar una amplia evolución del sistema de drones, no sólo en su uso militar, ya que también han sido utilizados para otros fines, como la visualización de entornos para la realización de mapas, observaciones atmosféricas y terrestres, la siembra de arroz y la fumigación, es preciso dar cuenta de que el proceso para su regulación ha dependido de los marcos o paradigmas del contexto beligerante y de confrontación en la política internacional más que de sus avances técnicos. Es decir, “el dispositivo no tiene la culpa de ser usado con fines de vigilancia y control de las sociedades tomadas como enemigas”.[73]

Atendiendo a la clasificación de los drones, esta se ha hecho con base en las distintas formas de operarse y a las características de cada uno. Véase la siguiente tabla de elaboración propia con información tomada del trabajo realizado por la Consejería de economía y hacienda de Madrid.

---

[72] *The radioplane OQ-2 aereal targer drone was the first quantitaive UAV purchase for the Unitad States*. Military Factory. [En línea]. http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=331. [Página consultada el 019/ II/ 2019.

[73] *Los Drones y sus aplicaciones en la Ingeniería Civil*. Madrid. [En línea*] https://www.fenercom.com/wp-content/uploads/2015/03/Los-Drones-y-sus-Aplicaciones-a-la-Ingenieria-Civil-fenercom-2015.pdf*. [Página consultada el 04/ II/ 2018].

Tabla 4. Clasificación de los drones

Modo	Explicación
Manual	El piloto remoto actúa sobre las superficies de control a través de una emisora de radio control.
Autónomo	Se establece un plan de vuelo y una vez iniciado, la nave ejecuta el plan de manera autónoma, no requiere la intervención de piloto incluso en situaciones de emergencia.
Asistido	El piloto remoto no actúa directamente únicamente es utilizado para asistir a que dirección debe ir desde un puesto de radiocontrol.
Automático	La aeronave cuenta con un piloto y se traza una ruta de vuelo punto por punto y el piloto ejecuta el plan además de que mantiene el control y puede modificar los puntos del plan en todo momento.

Fuente: *Los Drones y sus aplicaciones en la Ingeniería Civil*. Madrid. [En línea*] https://www.fenercom.com/wp-content/uploads/2015/03/Los-Drones-y-sus-Aplicaciones-a-la-Ingenieria-Civil-fenercom-2015.pdf*. [Página consultada el 04/ II/ 2018].

Por tanto, a pesar de que los drones han tenido constantes modificaciones en los últimos años, mantienen un desarrollo progresivo para proporcionar calidad en la imagen a grandes alturas, cuentan con sensores y *software* a prueba de errores humanos. Entonces, hay que reconocer que, "los drones, están representando una revolución socio-militar posmoderna, son una progresión de largo alcance que residen en la relación de cada momento histórico. Las consideraciones que se le dan a un dron van desde la eficiencia hasta las consideraciones éticas de uso".[74].

En este punto, se puede cuestionar: ¿por qué interesaría a la disciplina de las Relaciones Internacionales el avance tecnológico de los UAV? Una primera respuesta es que, las regulaciones legales siempre han ido detrás de la evolución de las nuevas tecnologías, aunque nunca en sintonía con las regulaciones internacionales sobre el uso de Vehículos No Tripulados, pues estos han tomado cada día más fuerza y, la constitución de los mismos ha dejado ver ventajas contra las plataformas tripuladas para muchos otros usos.

En síntesis, se puede decir que, los drones han ido evolucionando con los años, registrando distintas etapas y siendo modificados dada la época y las necesidades políticas

[74] *El arma de moda: Impacto del uso de los drones en las Relaciones Internacionales y el Derecho Internacional Contemporáneo*. [En línea]. Dirección URL: http://icip.gencat.cat/web/.content/continguts/publicacions/arxius_icip_research/ICIP_RESEARCH-4_WEB.pdf [Página. consultada el 27/I/2018].

y/o militares. El primer dron construido en Estados Unidos era un globo aerostático con mecanismo de bombardeo, cargaba con explosivos y un temporizador, el ataque se soltaba calculando las distancias y el viento además del ajuste de tiempo, recibió el nombre de Bombardero Aéreo de Perly. A pesar de ser un dispositivo bastante elaborado fueron nulos los resultados ya que la precisión no era buena ni constante.

Durante la Primera Guerra Mundial, apareció en Estados Unidos el primer dispositivo UAV, este era llamado *Sperry 14*; tenía mucha mejor precisión y era únicamente para combate, se inventó además un giróscopo que ayudaba a mantener un vuelo estable y nivelado.

Figura 2. Imagen del Sperry14. [75]

Fuente: *Los Drones y sus aplicaciones en la Ingeniería Civil*. Madrid. [En línea*] https://www.fenercom.com/wp-content/uploads/2015/03/Los-Drones-y-sus-Aplicaciones-a-la-Ingenieria-Civil-fenercom-2015.pdf*. [Página consultada el 04/ II/ 2018].

Esta nave podía cargar hasta 300 libras de bombas, sin embargo, nunca se utilizó en combate hasta que en 1918 se diseñó un avión al que se llamó *Kettering Bug* el cual estaba hecho de madera y lienzo. Fue diseñado para salir, desde un auto con ruedas y despegar las alas dirigiéndose a un objetivo.

[75] *Ibidem.*

Figura 3. Imagen del Kettering Bug.

Fuente: *First cruise missile- Kettering´s Bug*. [En línea]. https://travelforaircraft.wordpress.com/2011/04/01/first-cruise-missile-%E2%80%94-the-kettering-bug/. [Página consultada el 03/ VIII/ 2018].

Para el año de 1935 se fabricó la llamada Abeja Reina (*Queen Bee*) y en esta ocasión fue diseñada en Reino Unido, para utilizarse en misiones de entrenamiento. Su estructura era de madera y tenía un control de radio. Su altura alcanzaba los 17000 pies y estuvo presente hasta el término de la II Guerra Mundial[76].

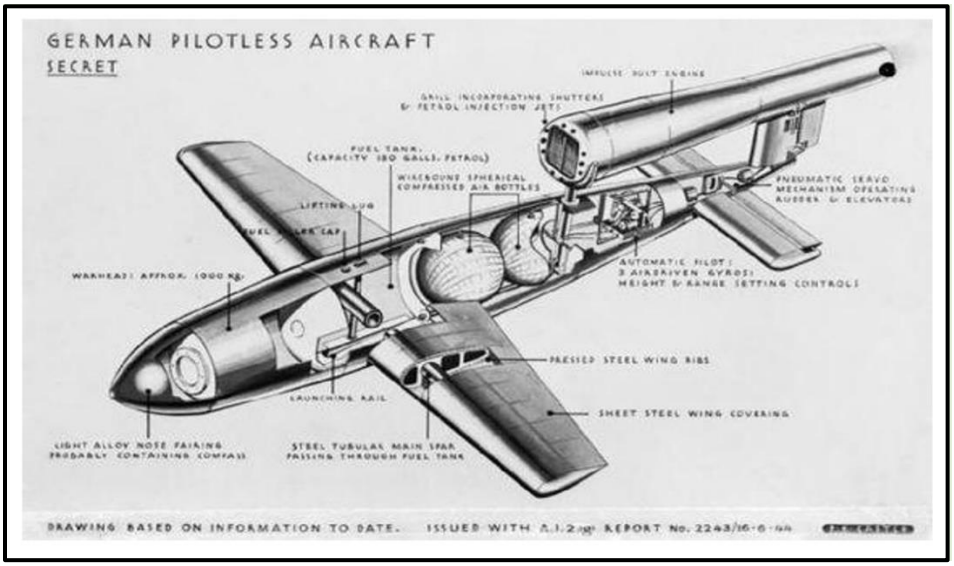
Figura 4. Abeja Reina (*Queen Bee*).

Fuente: *Rise of the Reapers: A brief history of Drones*. [En línea]. https://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones/. [Página consultada el 03/ VIII/ 2018].

[76] *Op. Cit.*

Para 1939, un británico fundó la Compañía *Radioplane Company, Northrop/Grumman* y "Alemania respondió con la fabricación de un nuevo UAV que básicamente para Hitler era una bomba voladora la cual buscaba ser utilizada contra objetivos no militares y es como se diseñó la Fi-103 conocido coloquialmente como *Vergeltungswaffe-1*".[77]

Figura 5. Imagen del *Vergeltungswaffe*.



Fuente: *V1 Reichenberg*. [En línea]. http://www.v1-reichenberg.com/geschichte_d.html. [Página consultada el 04/ VIII/ 2018].

Vergeltungswaffe-1 tenía un pequeño motor que emitía un ruido parecido a un zumbido, cargaba aproximadamente 2,000 libras y podía ser programado para viajar aproximadamente 150 millas. Se utilizó por primera vez en la Gran Bretaña con una desafortunada efectividad de 900 civiles muertos y más de 30,000 personas heridas[78].

Para la década de los 60´s EE.UU. actualizó su plan de ataque mediante los UAV ya que tenían una notable diferencia en comparación con los alemanes. Lo primero fue promover una misión de reconocimiento y, para ello utilizaron un prototipo de nombre *Firebee,* el cual, tenía bombas para su liberación en objetivos terrestres. Debido al éxito de este prototipo, estuvo en el mercado durante varios años y con diferentes modificaciones adaptadas a las necesidades de épocas, algunos permanecen aún activos con una señal de GPS, su producción fue vasta y es fue considerado como el primer UAS a pesar de que en un principio no era reconocido como tal.

[77] Traducido al español como *Arma de Venganza*.
[78] *Op. Cit.*

A finales de 1980 la inteligencia de Israel construyó un *UAV Pioneer* mismos que fueron comprados por Estados Unidos, convirtiéndose estos drones en los más pequeños de su época además de equipados. Podían despegar de tierra o mar y eran económicos. Se usaron para vigilancia por el Golfo y Bosnia y Medio Oriente.

Figura 6. Imagen del *UAV Pioneer*.

Fuente: *AAI RQ-2A Pioneer — first UAV to accept a military surrender*. [En línea]. https://travelforaircraft.wordpress.com/2012/04/20/aai-rq-2a-pioneer-write/. [Página consultada el 05/ VIII/ 2018].

“También estos años tuvieron la llegada del primer dron japonés llamado *Vertical Take-Off and Landing* (VTOL). En este caso el tema militar se dejó de lado y se utilizó este modelo para la siembra de arroz y fumigación, teniendo gran éxito.

Figura 7. Imagen del VTOL.

Fuente: *Aplicaciones Civiles de los Vehículos Aéreos No Tripulados (VANT) / Unmanned Aerial Vehicles (UAV*). [En línea]. http://www.aviacioncivil.com.ve/aplicaciones-civiles-de-los-vehiculos-aereos-tripulados-vant-unmanned-aerial-vehicles-uav. [Página consultada el 08/ VIII/ 2018].

Ante las situaciones de tecnología, Europa estaba un poco atrasada en la dinámica de los drones, oportunamente el mercado lo mantenía Israel y Estados Unidos por lo que España decide experimentar en el tema y desarrolló un programa llamado Avión Táctico de Largo Alcance No Tripulado español (Atlante) que, si bien no era un dron era un programa especializado para ellos. El Atlante puede ser elevado por tierra, aire o mar, recuperado mediante paracaídas y sus actividades están dirigidas a la lucha antiterrorista, contra la migración, lucha contra incendios y desastres naturales, así como supervisión de daños, vías de comunicación e infraestructuras.

Figura 8. Imagen del UAV Atlante.

Fuente: Airbus Defence and Space. [En línea]. https://airbusdefenceandspace.com/wp-content/uploads/2016/07/atlante-brochure.pdf. [Página consultada el 10/ VIII/ 2018].

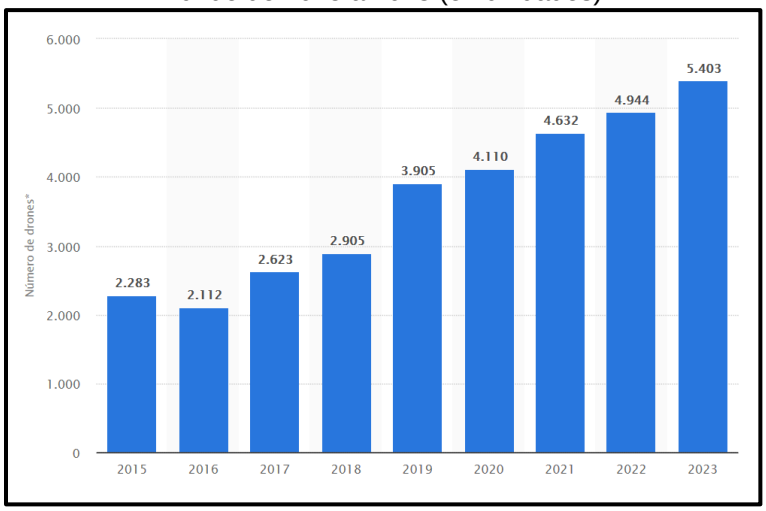
Así, con el avance tecnológico, a partir del **UAV** español, se han ido comercializando otros tipos de drones como el *Mikrokopter* en diferentes versiones. Considérese que, existen drones construidos del tamaño de la mano. Su control puede ser llevado a cabo mediante controladores lineales, tienen GPS, control máximo de altura, y el sistema vuelve a casa, aterrizando con seguridad.

Figura 9. Imagen de un *Mikrokopter*.

Fuente: *Airbus Defence and Space*. [En línea]. https://airbusdefenceandspace.com/wp-content/uploads/2016/07/atlante-brochure.pdf. [Página consultada el 10/ VIII/ 2018].

Sin duda alguna, la iniciativa de seguir con la fabricación de drones es evidente, y, en los últimos diez años su producción ha crecido de manera exponencial, aunado a que se vaticina siga esa tendencia, como lo señala la siguiente gráfica.

Gráfica 1. Previsión del volumen de producción de vehículos aéreos no tripulados militares en el mundo de 2015 a 2023 (en unidades).



Fuente: *Previsión del volumen de producción de vehículos aéreos no tripulados militares en el mundo de 2015 a 2023.* [En línea]. https://es.statista.com/estadisticas/658877/prevision-de-fabricacion-mundial-de-drones-militares/. [Página consultada el 23/VI/2019].

Como señala Velázquez Olivera, "se han hecho prototipos de drones para enviar ayuda médica inmediata, además que, los drones han causado gran furor últimamente porque son aeronaves pequeñas que pueden controlarse fácilmente desde un teléfono inteligente y porque son capaces de portar cámaras u otros dispositivos y sensores eléctricos" [79], como lo muestran las figuras 10 y 11.

Figura 10. Prototipo de dron ambulancia capaz de llevar un desfibrilador en un tiempo récord

Fuente: Presentan "dron ambulancia" capaz de transportar desfibrilador. [En línea]. https://www.telemetro.com/tecnologia/2014/10/28/presentan-prototipo-ambulancia-transportar-desfibrilador/1682396.html. [Página consultada el 25/VI/2019].

[79]Ana Velázquez Olivera. *El mundo de los drones*. [En línea]. www.cienciorama.unam.mx/a/pdf/538_cienciorama.pdf. [Página consultada el 23/VI/2019].

Figura 11. Águila entrenada para cazar drones

Fuente: ¿Pueden las águilas cazar drones? [En línea]. https://www.eulixe.com/articulo/imagen/pueden-las-aguilas-cazar-drones/20190305101351010226.html. [Página consultada el 23/VI/2019].

Para concluir la sección, es necesario hacer mención que Ana Velázquez nos muestra como el uso de los drones ha pasado de lo estrictamente militar a lo civil:

> "Son cada vez más comunes y pueden implementarse con sensores y equipo extra para un uso específico. Por ejemplo, los hay enfocados en el mapeo e imágenes terrestres, en la agricultura, inspección y monitoreo, entrega y transporte de toda clase de productos, y entretenimiento. Hay compañías que se dedican específicamente a la creación de hardware y al diseño de drones con radares para crear mayor autonomía, incluso los hay que pueden navegar sin que alguien los controle de manera remota. Además, hay quienes se dedican a la gestión del espacio aéreo de los drones, a asegurarlos y a conectar a clientes con operadores de drones según sus necesidades y cercanía"[80].

Figura 12. Nuevos usos de los drones

[80]Ana Velázquez Olivera. *El mundo de los drones*. [En línea]. www.cienciorama.unam.mx/a/pdf/538_cienciorama.pdf. [Página consultada el 23/VI/2019].

Fuente: Ana Velázquez Olivera. *El mundo de los drones*. [En línea]. www.cienciorama.unam.mx/a/pdf/538_cienciorama.pdf. [Página consultada el 23/VI/2019].

2.2.2. *Big Data*

Gracias a la cantidad de datos recibidos en el mundo surge en el año 2000 el término *Big Data* o mejor llamado Datos Masivos. Actualmente, los datos que las personas registran día con día en dispositivos son de fácil acceso y rastreo, ya que no se necesita más que una computadora o un teléfono móvil. Así, el término *Big Data* se ha vuelto importante, siendo la tendencia en la tecnología, esto es, un nuevo enfoque que se utiliza para recibir gran cantidad de datos que son casi imposibles de cargar en bases de datos.

La idea de que la información contenida no cabía en ningún lugar más, llevó a los ingenieros a resolver el problema mediante una herramienta capaz de procesarla, los términos utilizados para contabilizar la información actualmente son los exabytes, estos se refieren a una gran escala para crear nuevas formas de valor. Así, los datos que actualmente se contabilizan en el mundo son: aplicaciones celulares como *Facebook, Twitter, WhatsAp*p, programas de televisión, libros digitales, *GPS*, correos electrónicos, llamadas telefónicas, medidores eléctricos, cartas del correo postal, música, video, sensores, cambios en el aire, radios, fotografías, velocidad, entre algunas otras. De esta manera, los datos masivos cuentan con una clasificación específica.

- Medios de comunicación: se refiere principalmente a las redes y aplicaciones sociales como *Facebook, Linkedin, Twitter, Instagram, Snapchat*.
- Máquina a máquina: medios que te permiten conectarte a otros dispositivos mediante redes inalámbricas por ejemplo los velocímetros, variables meteorológicas, termostatos, variables químicas y de salinidad.
- Gran transacción de datos: por ejemplo, el efectuado por el Servicio de Administración Tributaria (SAT), mediante el registro de facturación. También se encuentran los registros de llamadas y telecomunicaciones.
- Biométricas: información de huellas digitales, escaneo de retina, reconocimiento facial, temas de genética, normalmente estos eran utilizados en las agencias de investigación, sin embargo, ahora ya podemos relacionar el ejemplo claro con IPhone y su escaneo de retina.

- Generada por el humano: estas son principalmente en llamadas o en los centros de trabajo llamados *Call Center*, se establecen llamadas de voz, notas y correos electrónicos, así como claves y números de seguridad de tarjetas personales".[81]

Además, debe considerarse que, los datos masivos, son también consecuencia del llamado Spam, esto es, mensajes publicitarios que están normalmente presentes en el correo electrónico, en aplicaciones y/o juegos en línea, cuyos filtros están diseñados para adaptarse a la medida de la búsqueda realizada. Es decir, si el usuario efectúa una búsqueda sobre ciertas compras, después podrá encontrar ofertas o mensajes relacionados con ella en otros medios de comunicación.

Un ejemplo básico del uso de los datos masivos es el caso de Google, quien cuenta con el mejor traductor a nivel mundial, en este momento tiene poco más de 70 idiomas diferentes y todo esto es gracias a *Big Data*. La explicación es sencilla, logró organizar de una forma básica y accesible para todo el mundo los datos acumulados en su página, sus creadores realizaron un protocolo preciso, se juntaron todas las palabras inglesas, por ejemplo (o de cualquier idioma), con y sin errores y se integraron a la herramienta de traductor. Los creadores comentan que la fórmula era económica ya que, gracias a los mega datos obtenidos en la página podían juntar oraciones bien redactadas. Hasta ahora es el más cercano a la traducción perfecta, tienen la mejor reducción de error y cada día abarcan más idiomas internacionales[82].

Amazon, por ejemplo, comenzó con venta de libros al público, gracias a los datos compilados eran capaces de saber cuánto tiempo el lector miraba el libro a comprar, qué tipo de libros buscaba o le interesaban y de esa manera arrojaba algunas recomendaciones extras. Fue tal su éxito, que hasta ahora Amazon es uno de los portales más importantes para realizar compras por *internet*. En este sentido, tómese en cuenta que:

> Amazon ha diseñado dispositivos como el *Kindle*, dispositivo mediante el cual puedes acceder a libros gratuitos o con costo, semeja páginas del libro y ha solicitado a algunos autores que incluso su versión solo pueda usarse mediante este equipo electrónico. Amazon ha datificado libros, sin embargo, no ha podido utilizarlos de la

[81]Ricardo Barranco. "*¿Qué es el Big Data?*" [En línea]. https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/. [Página consultada el 8/II/2018].
[82] Viktor- Schonberger Mayer, Kenneth Cukier. *Big Data. La revolución de los datos masivos*. Turner Editorial, España, pp.195-196.

manera en que Google lo hace para uso y beneficio propio, dando lugar a un mayor crecimiento tecnológico[83].

Atendiendo a la datificación, se sabe que, el tema de los GPS son parte también importante del término. La geolocalización arroja números importantes. Así, gracias a los satélites el ser humano puede saber la ubicación de personas, chips, automóviles, teléfonos, etc. *Google, Apple y Microsoft* han creado sus propias aplicaciones de localización. Para *Google* es conocido su vehículo *Street View*, iPhone por su parte, actúa como *espía* sin que el usuario esté conscientes de ello. Además, empresas como *UPS y DHL* instalan chips de rastreo y cámaras para monitorear tanto a sus empleados como a las camionetas repartidoras y de carga. Aplicaciones actuales como *Waze* son capaces de mostrar en tiempo real cualquier accidente, atasco de tráfico, alcoholímetro y demás situaciones en la calle.

Otras aplicaciones como Twitter permiten la datificación de sentimientos mediante sus hashtags, algunas otras pueden demostrar mediante ritmos cardiacos si se ha contraído gripe o cuántas personas en el grupo de trabajo se han contagiado, *Linkedin* datifica experiencia profesional y, *Facebook* datifica reacciones a publicaciones, noticias y artículos. Port su parte, *Apple* es capaz de datificar el ritmo cardiaco, temperatura, oxigenación de la sangre, cantidad de km recorridos y demás síntomas corporales a través de su aplicación *Healthy* en cada *iPhone, IPod, y Iwatch* comprado. Por tanto, gracias a toda esta datificación, algunas empresas han sido capaces de analizar la información en beneficio propio, por lo que, debido a los datos masivos, el mundo es una sucesión de acontecimientos totalmente explicables[84].

En síntesis, entiéndase al *Big Data* como lo hace la empresa *Gartner*, dígase "aquellos recursos de información caracterizados por su alto volumen, velocidad o variedad, que requieren formas de procesamiento innovadoras y eficientes para la mejora del conocimiento y la toma de decisiones".[85]

Por tanto, con base en la página de *Logicalis,* las características que definen el *Big Data* pueden resumirse en lo que se conoce como las tres Vs: Volumen, Velocidad y Variedad.

Volumen. Se considera que en 2020 más de 25 mil millones de dispositivos estarán conectados a Internet, acrecentando un volumen de datos que a finales de 2013 ya se estimaba en 4,4

[83] *Op. Cit.* Datificar: Se refiere a recopilar la información y medirla gracias a la infraestructura tecnológica. Crea caminos y vías de análisis, generalmente es utilizado por las empresas con los datos recogidos que utilizan para fines en concreto.

[84] *Ibidem.*

[85] Estrella Pulido Cañabate. *Big Data: ¿solución o problema?* [En línea]. http://arantxa.ii.uam.es/~epulido/bigdata.pdf [Página consultada el 24/VI/2019].

billones de GB y que llegará, según los pronósticos, a multiplicarse por 10 en tan solo 6 años. Por supuesto, el impacto que tendrá este crecimiento exponencial del **volumen** de datos contenidos en *Big Data* sobre la inversión en TIC dará mucho que hablar en un futuro muy cercano.

Velocidad. La velocidad en el acceso y el flujo de datos es el gran reto que plantea *Big Data* no solo hoy, sino también —y, sobre todo— de cara al futuro. El indudable valor que aporta a los proyectos de *Business Intelligence* está determinado por sus tres «V», el manejo de las cuales pone encima de la mesa cuestiones de tanta importancia como, por ejemplo, si las herramientas de almacenamiento tradicionales deben quedar a un lado para dar paso a sistemas de gestión que no pretendan capturar datos indiscriminadamente para su posterior tratamiento y estructuración, sino que realicen esta tarea en tiempo real captando únicamente aquellos datos que aporten valor a los sistemas

Variedad. Efectivamente, el valor de *Big Data* no se agota con la mera consideración de su volumen: también la variedad de los datos que contiene es una de sus grandes riquezas. Pero además de abrir las puertas a nuevas oportunidades de negocio, ambas magnitudes también plantean uno de los grandes retos que actualmente afrontan las TIC: gestionar un volumen y una variedad ingente de datos facilitando el acceso inmediato a los mismos[86].

Cabe señalar que, el concepto de *Big Data* se ha venido definiendo y caracterizándose con base en tres dimensiones citadas. Sin embargo, en la actualidad también se habla de dos V's más, esto es, Veracidad y Valor.

Una de las características asociada a la calidad de los datos es la veracidad de los mismos. La veracidad puede entenderse como el grado de confianza que se establece sobre los datos a utilizar. Dentro de la caracterización del *Big Data* la veracidad determina su cuarta dimensión, y es de gran importancia para un analista de datos, ya que la veracidad de los mismos determinará la calidad de los resultados y la confianza en los mismos. Por lo tanto, un alto volumen de información que crece a velocidad muy rápida y basada en datos estructurados y desestructurados y provenientes de una gran variedad fuentes, hacen inevitable dudar del grado de veracidad de los mismos. Por ello, dependiendo de la aplicación que se les dé, su veracidad puede ser imprescindible o convertirse en un acto de confianza sin llegar a ser vital[87].

---

[86] *Procesamiento masivo de datos: volumen, variedad y velocidad, magnitudes y nuevos retos del Big Data*
[En línea] https://blog.es.logicalis.com/analytics/velocidad-variedad-y-volumen-las-3-magnitudes-clave-de-big-data. [Página consultada el 24/VI/2020].

[87] *Las 5 V y que sirven para explicar el Big Data*. [En línea]. https://www.master-bigdata.com/big-data-5-v/#:~:text=La%20veracidad%20puede%20entenderse%20como,la%20confianza%20en%20los%20mismos. [Página consultada el 24/VI/2020].

Desde el punto de vista de la recolección y explotación, la dimensión valor representa el aspecto más relevante del *Big Data*".[88]

Se dice que, actualmente "el valor marginal de los datos se representa gráficamente. En la siguiente gráfica se observa que, a medida que aumenta el volumen y complejidad de los datos, su valor marginal disminuye considerablemente, debido a su dificultad de explotación"[89].

Pero ¿cuál es el reto de *Big Data*? Se puede decir que, ante la generación que se hace cada día de un mayor volumen de datos (redes sociales, redes inalámbricas, telefonía móvil, nuevos servicios de almacenamiento en la nube, etc.,) provenientes de pocos o muchas fuentes de información, cuya veracidad es difícil de constatar, y cuyo tiempo de validez puede no ser muy grande, ante este tipo de escenarios, el llegar a verlos, no como una dificultad, sino como una ventaja competitiva es uno de los retos actuales de la implantación de la tecnología asociada al concepto de *Big Data*[90].

2.3. *Filtraciones de información. (Caso WikiLeaks)*

A partir de los acontecimientos en el año 2010 con el caso de WikiLeaks se da a conocer el termino "fuga de datos" o también nombrada "filtración de información" misma que se refiere a la pérdida de información ya sea de una Organización No Gubernamental, una empresa privada o de cualquier individuo.

Las fugas de datos pueden ser ocasionadas por causas internas o externas a las organizaciones:

- Internas: causadas, por ejemplo, intencionada o accidentalmente por personal interno de la organización.
- Externas: por ejemplo, la filtración de los datos personales de los empleados de una empresa por un incidente de seguridad de un proveedor.

Además, pueden ser deliberadas o involuntarias:

- Deliberadas: se filtran o revelan datos confidenciales con el propósito de obtener una ventaja económica o causar un daño o perjuicio a las organizaciones: sanciones económicas, la pérdida de una ventaja competitiva, la pérdida de imagen o reputación, etc.

---

[88] *Big Data Future. Los Small Data: La última milla del Big Data*. [En línea]. https://bigdata400.wordpress.com/ [Página consultada el 24/VI/2019].
[89] *Las 5 vs que caracterizan el concepto de Big Data.* [En línea]. https://www.vision*software*.com.co/las-5-vs-que-caracterizan-el-concepto-de-big-data/. [Página consultada el 24/VI/2020].
[90] *Ibidem*

- Involuntarias: se filtran o revelan datos confidenciales de manera accidental o no intencionada, por ejemplo, por no seguir las buenas prácticas de seguridad de la información[91].

Para ahondar un poco más en este tema, este capitulo habla de la filtración de información a través del ya mencionado caso WikiLeaks. Esta plataforma se describe a sí misma como una fundación de rubro Internacional conformada por personas con profesiones técnicas, matemáticas, científicas y comunicólogas. Su lanzamiento fue en diciembre de 2006 sin embargo, su actividad comenzó en julio de 2007. *WikiLeaks* aparece en una nube informativa a nivel internacional, desde entonces y hasta ahora, ha provocado discusiones en los ámbitos sociales y políticos.

No obstante, surge como una amenaza internacional al periodismo como se le conocía hasta entonces, superó en calidad y volumen a cualquier periódico físico o virtual en existencia. Su fundador y desarrollador es Julián Assange quien fue la primera persona en hacer filtraciones masivas por medio de *internet*.

La historia de *WikiLeaks* comienza con un hacker que intercambió correos con otras instituciones y otros hackers, operado únicamente por un servidor y dos personas, Assange y su colaborador Domscheit-Berg. Así, sin mayores ingresos más que sus propios fondos, lograron realizar una página que atemoriza a empresarios y políticos por igual.

El modo de operación era el siguiente. En primer término, la información podía ser colocada en la página de manera anónima y, posteriormente, se verificaban los documentos que llegaban para saber si la información había sido manipulada técnicamente. Luego, se realizaba una copia de seguridad y mediante pesquisas de información y confianza se publicaba el artículo. Cabe señalar que, el medio en el que se dio a conocer *WikiLeaks* consideraba que las personas detrás del tema tenían toda una red de informática, que contaban con grandes fondos económicos además de un equipo profesional para la revisión de la información. El mismo Assange cita:

> Las fuentes que proporcionaron información a esta plataforma son hasta ahora anónimos, sin embargo, hay quien comenta que es toda una treta por parte del mismo gobierno estadounidense para imponer escenarios necesarios en la política (caso Guerra contra el Medio Oriente y el caso de la guerra contra el terrorismo a partir del 11 de septiembre de 2001)[92].

[91] ¿Qué es la fuga de información? [En línea]. https://www.bancosantander.es/glosario/fuga-datos. [Página consultada el 24/VI/2021].
[92] Julian Assange. *Cuando Google encontró a WikiLeaks*. Capital Intelectual. Estados Unidos, pp. 35

Pero surge una pregunta, ¿cómo es posible que solamente dos personas tengan la capacidad para tener un millón de documentos? Existen dos creencias, la primera que Assange mantenía filtración en archivos de periodismo, además de filtraciones de otros periodistas con responsabilidad de publicar cierta información. La segunda es que normalmente *WikiLeaks* anunciaba que la información provenía de tres fuentes independientes, sin embargo, su colaborador desmintió esto después, re-aclarando que no conocen las fuentes de ninguno de sus documentos exhibidos y no son capaces de localizarlos ni identificarlos.

Para Ramón Tijeras, a este tema le mantuvieron ciertos límites de seguridad, pues se trataba de revisar la información antes de publicarla; sin embargo, debido a la cantidad de la misma les era casi imposible. Por eso, uno de los límites fue evitar poner el nombre de las personas detrás de *WikiLeaks* ya que cualquier persona que apareciera publicada en la Web sería capaz de localizarlos. Así, considérese que:

> El modus operandi entonces era más sencillo, ellos podían publicar la información sin ser localizados, personajes como Manning ayudaron a transmitir mucha de esta gracias a su cercanía con el gobierno estadounidense. Este personaje logró filtrar más de 250,000 cables diplomáticos que pusieron en jaque la política internacional[93].

Se sabe que, la información se grababa hasta que se envió a un periodista quien lo delató ante el gobierno de Estados Unidos y se procedió a su detención. Manning fue sentenciado por difundir información confidencial a *WikiLeaks*, sin embargo, no se tenía la certeza de que eso fuera así. *WikiLeaks* reaccionó de inmediato y publicó que apoyaría con los gastos de defensa de Manning, pero hasta ahora no se sabe si realmente que sucedió así ya que solo se confirmó una pequeña ayuda durante su proceso.

Así como *WikiLeaks* pasa de ser un portal en la web a tener un trabajo como el de periodistas para la difusión de información, Assange quien ya tenía experiencia en estos temas de seguridad, consideró que, aunque ellos publicarían la información, la sociedad podría creer que no era lo suficientemente viable. El método fue sencillo: primero realizaban la revisión del documento como cualquier medio de comunicación, se editaba y se tomaba lo más importante o digerible para el público.

Recuérdese que, en el año 2007 *WikiLeaks* provocó una revuelta en los medios por la edición del video llamado *Asesinato Colateral*. En el video se muestra la muerte de 12

[93] Ramón Tijeras. *Comunicación 21. WikiLeaks, el periodismo tradicional y las nuevas plataformas de información*. [En línea]. http://www.comunicacion21.com/de-*WikiLeaks*-a-openleaks-la-crisis-de-los-medios-y-las-nuevas-plataformas-de-informacion/. [Página consultada el 08/ I/ 2018].

personas, además de 2 menores de edad heridos de los cuales no se tiene más información. El resumen de los sucesos es el siguiente:

> En Iraq desde un helicóptero estadounidense se visualizan personas caminando con algo al hombre que identifican como armas de alto calibre, al sentirse "amenazados" solicitan permiso para abrir fuego el cual es concedido. El ataque dura aproximadamente dos minutos en dos escenas continuas de ráfagas, cuando ninguna de las personas parece moverse, llega una camioneta por los cuerpos, el helicóptero abre fuego nuevamente y termina con la vida de las personas de la camioneta. Los refuerzos por tierra llegan al evento confirmando la muerte de 12 personas e intentan llevar a los dos menores al hospital ya que se encontraban dentro de un vehículo, la certeza de este ataque fue contundente a nivel internacional ya que las personas quienes parecían portar armas era un fotógrafo de *Reuters* con cámaras profesionales al hombro, su nombre: Namir Noor-Eldeen[94].

Muchos trataron de rastrear y obtener el vídeo, pero sólo Assange lo obtuvo y gracias a la ayuda de periodistas se logró exhibir el vídeo en los más grandes canales de televisión Internacional. Se dice que fue el mismo Manning quien lo proporcionó a *WikiLeaks*. ¿Quién conforma *WikiLeaks*? Desde el punto de vista académico se visualiza como una organización establecida por el mismo gobierno estadounidense, ¿la razón? algunos de los integrantes son exiliados chinos que estuvieron inmiscuidos en temas de la CIA.

El modo de financiación nadie lo conoce, se tienen suposiciones al respecto tales como Cryptone.org, un sitio web con precedentes a *WikiLeaks* ha dado a conocer que existen fundaciones que dan financiamiento a la web dentro y fuera de Estados Unidos.

A pesar de que su fundador ha solicitado apoyo económico se cree que mantiene información clasificada que podría vender a altos costos para lograr el financiamiento del sitio, sin embargo, en febrero del 2011 Reuters anunció que *WikiLeaks* estaba incapacitado para seguir recibiendo información. Lo cierto es que siempre existirán filtraciones de información, algunas veces los hackers se inmiscuyen en las computadoras de periodistas que tienen información especial para su edición, posteriormente se da a conocer la misma sin embargo siempre existe el riesgo de que alguien más la pueda obtener.

También hay certeza que la mayor parte de información está editada para establecer los límites con la que la sociedad la recibirá. La información en pocas palabras siempre será controlada y ese es el motivo por el que *WikiLeaks* ha sido un contrataque a las elites empresariales y políticas. En este sentido, considérese lo siguiente:

---

[94] *WikiLeaks*. *Collateral Murder*. [En línea]. https://www.youtube.com/watch?v=teCB48QT1zs. [Página consultada el 12/ I/ 2018].

> Intelectuales han dado sus opiniones sobre *WikiLeaks*, han intentado explicar de una forma más específica como puede ser una manipulación gubernamental sobre la sociedad tal y como aseguran pasó con el 11 de septiembre. Por mencionar a uno más está Michael Choussudovsky quien estudia el caso del web centrado en Medio Oriente, comenta que se publicó más de un millón de páginas sobre Afganistán sin hacer mención del tráfico de drogas[95].

Por tanto, el impacto político y social que contrae este portal ha obligado de cierta manera a los medios de comunicación a realizar nuevas estrategias en el manejo de la comunicación. En la misma vertiente, otras páginas o sitios han declarado su apoyo total al uso de la información como hasta ahora la había llevado Assange.

El caso de Anonymous ha tenido injerencia en contra de empresas y gobierno como apoyo, tales como ataques contra Amazon, VISA y MasterCard quienes no tuvieron acceso a sus páginas de *internet* por algún tiempo. Se sabe que, a pesar de las diferentes acciones llevadas a cabo como protesta por la baja de la página, la misma sigue inaccesible, sin embargo, el colaborador de Assange dio paso a una nueva plataforma llamada *Openleaks*.

WikiLeaks por ahora permanece con información reciente en su página de *internet*, sus últimas publicaciones son del 2017. Su fundador Assange ha recibido premios por parte de universidades y en el año 2011 obtuvo el premio como Mejor Jornalista. En el 2012 se refugió en la Embajada de Ecuador en Londres y solicitó asilo político, mismo que le fue aceptado en el mismo año. El asilo se le otorgó debido a que Ecuador consideró que la persecución internacional que estaba realizando Estados Unidos era una violación a la Convención de Viena y según los términos de la ley internacional. esta debía ser concedida[96].

Ahora, ¿por qué se puede decir que *WikiLeaks* es un arma informática? Quien sustenta este trabajo, considera que, la respuesta es que *WikiLeaks* es una plataforma que recibe información anónima, por lo que la persecución se ha volcado a una completa investigación en torno al personal de *WikiLeaks*. Los mismos integrantes de este caso fueron perseguidos en diferentes países como Alemania, Islandia, Londres y Dinamarca por personal del gobierno de Estados Unidos. En el año 2014 el Departamento de Justicia

---

[95]Michael Choussudovsky. *Línea de Fuego. "Quién está detrás de WikiLeaks?* 2011. [En línea]. https://lalineadefuego.info/2011/01/25/%C2%BFquien-esta-detras-de-*WikiLeaks*-michel-chossudovsky/. [Página consultada el18/XII/ 2018].

[96] Julián Assange. *Cuando Google encontró a WikiLeaks*. Capital Intelectual. Estados Unidos, pp. 230.

de Estados Unidos, presentó una orden judicial para que el personal fuera detenido en cualquier aeropuerto.

Figura 13. Manning (izquierda), custodiado por otro soldado, en Fort Meade (EE.UU.), el 22 de diciembre del 2011.

Fuente: Así fue el caso *WikiLeaks*. [En línea]. https://www.elperiodico.com/es/internacional/20170118/asi-fue-el-caso-*WikiLeaks*-5750289. [Página consultada el 09/ II/ 2019].

A la saña, se suma el caso de Chelasea Manning quien estuvo detenida, fue violentada y torturada con el fin de obtener información sobre el tema y relación con *WikiLeaks*. Fue acusada por ser la fuente periodística y a pesar de que dio una declaración voluntaria de culpa, su sentencia fue de 35 años en prisión sin posibilidad de disminución, a pesar de haber sido obligada a aceptar el trato con el gobierno estadounidense. Como se supo: "muchos empresarios y políticos ya solicitaban el asesinato de Julián Assange, fundador de *WikiLeaks* ya que lo identificaban como un terrorista de alta tecnología y combatiente enemigo implicado en una guerra tecnológica".[97]

De esta manera, el *internet* interrumpió permisos para *WikiLeaks*.org, sin embargo, otros servidores ofrecieron servicio de albergue para las publicaciones de *WikiLeaks*.

A nivel nacional, Estados Unidos realizó una prohibición clara con el tema, Obama envío una prohibición a empleados y estudiantes que visitaran los artículos o la página. La amenaza era que, quien quisiera conservar su trabajo o hacer una carrera como funcionario público, debían evitar a toda costa visitar este sitio o cualquiera de sus artículos. La campaña de sabotaje alcanzó a personajes importantes en el periodismo, las grandes

[97]Julian Assange. *Cuando Google encontró a WikiLeaks*. Capital Intelectual. 2014. Estados Unidos. 221 p.

empresas de VISA y MasterCard denegaron los servicios, bloquearon tarjetas bancarias y transferencias[98].

El bloqueo bancario, que fue como se le llamó, alcanzó a países como Islandia quien falló a favor de *WikiLeaks* por considerar la situación como un abuso de dominio. Durante estos hechos, el gobierno estadounidense comenzó a enviar citatorios a Twitter para que entregara la información como cuentas, tarjetas personales, números de teléfono de involucrados o allegados. Se realizó un llamado a Facebook y Google por parte de *WikiLeaks* para que revelaran si a ellos les había sucedido lo mismo que a Twitter y en caso de dar una respuesta positiva solicitó que fueran informados, incluso el fundador de *WikiLeaks* contactó al fundador de Google para que le proporcionara información sobre el tema.

Sería interminable continuar analizando los hechos, causas y consecuencias de *WikiLeaks*, por tanto, haciendo un breve resumen de sus actividades, se puede decir lo siguiente:

> Lo que hay que enfatizar, una vez más, es que todos los Wiki-datos se redactan de forma selectiva y, a continuación, unos medios que sirven a las élites económicas los analizan e interpretan. Pese a que la numerosa información que contiene el banco de datos de *WikiLeaks* es accesible, el público más amplio no se tomará la molestia de consultar y revisar el banco de datos del grupo. El público leerá las selecciones redactadas y las interpretaciones que se presentan en los medios más importantes. De esta forma, se presenta una imagen parcial y tendenciosa. La opinión pública acepta la versión redactada porque se basa en lo que se anuncia como una fuente fidedigna cuando, de hecho, lo que se presenta en las páginas de los periódicos más importantes y en los canales de televisión no es más que una distorsión de la realidad cuidadosamente trabajada y enrevesada. *WikiLeaks* tiene las características de un proceso de disensión manufacturada. Busca denunciar las mentiras del gobierno. Ha revelado información importante en torno a los crímenes de guerra de Estados Unidos, pero una vez el proyecto se introduce en el molde del periodismo mayoritario, se emplea como instrumento de desinformación mediática[99].

2.4. Aplicaciones

Sin duda alguna, las aplicaciones en los equipos tecnológicos se han convertido en una herramienta capaz de proporcionar información exacta de cualquier aspecto de la vida de

[98] *Ibidem*, pp. 224.
[99] Ramón Tijeras. *Op. cit*. p.16

las personas. Por ejemplo, a partir de las descargas de juegos, aplicaciones, revisión de páginas o compras en línea en móviles o *tablets*, se está expuesto a ser revisado habitualmente, dando lugar a una relación que señala que, cuanta más información se tenga en los equipos, se podría decir que, se tiene menos seguridad informática. Esto lo confirma quien escribe un periodista que escribe para la Revista Tendencias al citar: "cualquier aplicación es capaz de acceder a diferentes recursos del teléfono, siempre que le autoricemos a ello".[100]

Ante estas situaciones, la Universidad Oberta de Catalunya (UOC) ha realizado una serie de recomendaciones a los usuarios, desde tipo de contraseñas hasta el uso de wifi público. En resumen, trata de ofrecer información a la sociedad sobre los riesgos que se tienen al descargar cosas por *internet*, a saber:

- No acceder a la cuenta bancaria desde un wifi público
- Se recomienda el protocolo WPA2 (Sistema que protege redes inalámbricas, no es pública y la información que proporciona parece ser poca)
- Recurrir a tiendas oficiales de las aplicaciones
- Reconocer que Apple mantiene una mejor seguridad que Google
- Leer los términos y condiciones de las aplicaciones que se descargan o de las páginas que se visitan
- Realizar constantes copias de seguridad en archivos y teléfono
- No tener demasiadas contraseñas y hacerlas seguras
- No dar a conocer la ubicación del equipo todo el tiempo (sólo cuando sea necesario)
- Recurrir a los sistemas de encriptación de información como, por ejemplo, WhatsApp[101].

Seguir el decálogo de seguridad informática proporciona conocimiento extra no ofrecido al usuario desde su adquisición.

> Probablemente, el libro de 1984 de Orwell parecía adelantado a su época, sin embargo, menciona en sus primeras páginas que cada persona en su domicilio debía tener un televisor en un lugar donde pudiera tener una vista general de la casa, esto tenía como objetivo, ver lo que hacían las personas a través de la pantalla y de esta manera confirmar su modo de vida. La ficción alcanzó la realidad cuando en el 2015 la empresa Vizio reveló que sus televisores cuentan con tecnología integrada para espiar a los usuarios. Los televisores básicamente grababan todo lo que los espectadores consumen, programas de TV, DVD, y todo lo que hacían

[100]Francesc Bracero. *Aplicaciones de espionaje*. [En línea]. https://www.ucm.es/data/cont/media/www/pag48257/UOC.pdf. [Página consultada el 09/ I/ 2018].
[101] *Ibid.*

> conectados a *Internet*. Todo lo recabado, tenía como objetivo ser vendido a empresas que necesitaran un acopio de datos[102].

Google por su parte, se maneja de una forma más funcional, un ejemplo claro lo aporta Ignacio Ramonet cuando cita:

> Todas las actividades de tu día se registran mediante Google Chrome quien por su parte envía esta información a Alphabet (La empresa matriz de Google) todo lo que hace el usuario en materia de navegación. Google Analytics elabora estadísticas muy precisas de las consultas de los internautas en el Red. Google Plus recoge información complementaria y la mezcla. Gmail analiza la correspondencia intercambiada, lo cual revela mucho sobre el emisor y sus contactos. El servicio DNS (Sistema de nombres de dominio) de Google analiza los sitios visitados, Youtube, el servicio de vídeos más consultado en el mundo, que pertenece también a Google y, por lo tanto, a Alphabet, registra todo lo que hacemos en él. Google Maps identifica el lugar en que nos encontramos, adónde vamos, cuándo y por qué itinerario. Adwords sabe lo que queremos vender o promocionar. Y desde que encendemos un smarthphone con Android, Google sabe inmediatamente dónde estamos y qué estamos haciendo[103].

Por tanto, se cree que, para el año 2030 las sociedades serán grupos a través de *Internet* y redes sociales. Una parte importante de tener la cantidad de datos que sea cuantificada y guardada hace que las empresas puedan reutilizarlos cuando sea. Google da una vez más la muestra de ello, al considerar que, todos los datos malos, incorrectos o inservibles pueden ser muy útiles. De ahí que Google tenga el mejor auto corrector del mundo, mejor que el de Microsoft. Entonces, gracias a toda la información incorrecta datificada en su portal, ha logrado compilar la información para proporcionar un auto corrector gratuito mundial. Así, todo tipo de empresas y negocios, comienzan a programar sus sistemas para recolectar información útil. Con base en ellos, pueden realizar excelentes estudios de mercado, establecer su falla y error y saber las preferencias de compra y visualización de sus clientes.

Sin embargo, a pesar de que se considera que los datos masivos no tienen ningún riesgo a la privacidad, tampoco se plantean leyes o reglamentos que impidan a los gobiernos mantener una red de mega datos sobre la población. La intimidad entonces es violada. Estados Unidos, es el país con mayor número de centros de compilación de datos,

---

[102] *Vizio podría atajar la recogida indebida de datos*. [En línea]. https://www.xatakahome.com/televisores/vizio-podria-atajar-recogida-indebida-datos-ofreciendo-notificacion-pantalla-a-usuarios-afectados. [Página consultada el 09/ IX/ 2018].

[103] Ramonet Ignacio. *El Imperio de la Vigilancia*. Editorial Clave Intelectual. Madrid. 2015. P. 82.

ahí recolectan diariamente información de los millones de usuarios con artículos tecnológicos, siendo justificación que “el gobierno nunca sabe a quién va a querer: escruta, recopila, almacena y garantiza el acceso a la información, no necesariamente para monitorizar a todo el mundo todo el tiempo, sino para que cuando alguien caiga bajo sospecha, se hallen en condiciones de investigar de inmediato en vez de tener que empezar a reunir información desde cero”.[104]

Pero ¿qué tendencias dominarán el futuro de las App’s? Véase la siguiente tabla elaboración propia con información tomada de Forbes. *Así serán las apps del futuro*. [En línea]. https://www.forbes.com.mx/asi-seran-las-apps-del-futuro/ [página consultada el 24/VI/2019).

Tabla 5. El futuro de las App’s.

Rasgo	Implicaciones
Sensores conectados a *internet*.	Lo interesante de los sensores, como los que usan los wearables y los *smartphones,* no son ellos en sí mismos, son cada vez más eficientes y más baratos, pero su verdadero valor reside en que estén conectados, es decir, en su participación en el denominado *Internet* de las Cosas. En Suecia, manejar sobre hielo es un tema muy importante porque puede desencadenar accidentes. “Volvo ya tiene sensores para detectar si hay hielo adelante, eso es bastante bueno para el que maneja, pero un humano tiene mejores sensores que el auto. Si ese sensor está conectado a la nube, y esa nube manda la notificación a un auto que va un kilómetro atrás, el valor comienza a tener un efecto de red.
La transformación de datos complejos en imágenes simples.	De acuerdo con datos de la firma de análisis *Gartner*, para 2020 habrá más de 26 millones de objetos conectados a la red. El secreto del futuro de estas aplicaciones es cómo se consigue transformar esas matrices de datos muy complejas, pero con una visualización extremadamente simple.
Nuevas interfaces.	En este caso, se estima que, en cinco años, las APIs, es decir, el esqueleto para desarrollar apps, serán inadecuadas y ya han comenzado a evolucionar. Un ejemplo es que Facebook lanzó su propio lenguaje abierto, *GraphQL*. Si la plataforma es muy usada, va a ser inadecuada para uso particular. Además, este elemento debe estar vinculado al open data por parte del gobierno y empresas, pues el acceso más fácil a datos permite que se pueda interactuar mejor con las necesidades de los consumidores en el desarrollo de apps. Un caso de éxito de apertura de datos para la firma ha sido la app de la liga de futbol mexicana, BBVA Bancomer, que ha registrado más de un millón de descargas, con 400,000 usuarios que ingresan los fines de semana, 35,000 simultáneos y envía 200,000 notificaciones por segundo.

[104]Viktor- Schonberger Mayer, Kenneth Cukier. *Big Data. La revolución de los datos masivos*. Turner Editorial, España, pp.195-196.

Fuente: Forbes. *Así serán las apps del futuro*. [En línea]. https://www.forbes.com.mx/asi-seran-las-apps-del-futuro/ [página consultada el 24/VI/2019).

Por tanto, antes de pasar a conocer algunos relevantes casos de espionajes, multicitados en los medios de comunicación, considérese lo que Facebook tiene a su alcance, señalado en la siguiente tabla a saber:

Tabla 6. Lo que Facebook sabe de la gente.[105]

***Facebook* lo sabe todo**. además de la información que se comparte, Facebook sabe y conoce los hábitos, todo esto depende del comportamiento que se tiene dentro de la red social, es decir, todo lo que se tenga ligado a la computadora y equipo telefónico. Esta aplicación tiene la capacidad de saber:

- La batería del celular
- Los movimientos del mouse en la computadora
- El operador de servicio del celular
- La marca y procesador de tu computadora y/o dispositivos a los que te conectas
- El espacio libre de almacenamiento de tus dispositivos
- La velocidad y compañía de *internet* que utilizas
- Buscadores instalados en tus dispositivos (*Chrome, Safari, Explorer*)
- Compras realizadas en cualquier plataforma
- Información de contacto, historial de llamadas y mensajes de texto.
- La cámara que usas y la configuración que le das
- Frecuencia y duración de tu actividad
- Aplicaciones de tu celular y nombres de archivos guardados
- Información de tus páginas de *Internet*
- Información de los dispositivos cercanos a ti o la red de conexión
- Ubicación y fecha
- Configuración de tu celular, GPS y demás aplicaciones
- Información de cuando estás en línea o desconectado de *Internet*
- Información de tus juegos y todo tipo de cuentas
- Cuando tu comentas o compartes información en cualquier post, inmediatamente descargan la información de tu contacto.

Fuente: *Te sorprendería saber lo que Facebook sabe de ti*. Washington. [En línea]. https://www.elimparcial.com/EdicionEnLinea/Notas/Internacional/25032018/1321015-Te-sorprenderia-saber-todo-lo-que-Facebook-sabe-de-ti.html. [Página consultada el 09/ IX/ 2018].

[105]*Te sorprendería saber lo que Facebook sabe de ti*. Washington. [En línea]. https://www.elimparcial.com/EdicionEnLinea/Notas/Internacional/25032018/1321015-Te-sorprenderia-saber-todo-lo-que-Facebook-sabe-de-ti.html. [Página consultada el 09/ IX/ 2018].

3. CASOS RELEVANTES DE ESPIONAJE

> Por supuesto que no se puede justificar esa intervención. Pero eso es irrelevante. En México nadie pide permiso para hacerlo.
>
> Eduardo Guerrero
> Exfuncionario de la Agencia de Inteligencia del gobierno mexicano.

Día tras día surgen nuevos casos de espionaje y vigilancia entre los países y hacia el interior de estos. Ello ha dado lugar a la existencia de una infinidad de casos que son publicados en la prensa, radio y televisión, además de las redes sociales. Por tanto, haciendo una selección de los casos más sonados de espionaje internacional, en este trabajo se mencionan los referentes a el caso Snowden; la Operación Aurora; el Caso *Echelon*; el Caso *Cambridge Analityca* y con respecto al entorno de nuestro país, se señalan el Caso del *Software Pegasus* y el de la periodista Carmen Aristegui y la Casa Blanca.

La selección de los mismos se realizó con base a la información y los casos más recientes del momento además de como se van relacionando conductualmente con los intereses políticos, económicos y sociales mismos que buscan obtener información de comportamientos, conductas, competencias e incluso datos personales realizando intervención mediante dispositivos que terminan por moldear comportamientos de las personas que se encuentran relacionadas con los mismos.

Los datos que se divulgaron a través de estos mecanismos de vigilancia o malware como normalmente se les llama, ha detonado en temas centrales como violación de Derechos Humanos, uso ilícito de información privada, acceso a dispositivos ilegalmente, nula intervención del gobierno para resolver el caso y/o aclarar la situación del uso de estos dispositivos.

El primero en detallarse es el caso Snowden ya que se puede decir que fue la primera persona que sacó a la luz documentos en los que se detallaba el modus operandi de estos malware contra la sociedad civil y las organizaciones por parte del gobierno estadounidense, a partir del momento de revelación no ha parado de salir información sobre el uso de los malware en distintos gobiernos y a través también para distintos objetivos y mediante múltiples usos.

Los casos de México llaman particularmente la atención ya que actualmente, es el segundo país de Latinoamérica que recibe ataques de malware según una investigación realizada por el equipo de Palo Alto quienes analizaron las amenazas en torno al tema año con año. Conocer estos temas es fundamental para a partir de ese momento se pueda saber que hacer en caso de robo de información o que acciones se deben tomar para

mitigar los ataques ya sean personales, empresas u organizaciones. A continuación, se detalla cada uno de los casos exponiendo como sucedió y cuáles al final del día eran los objetivos de cada uno de ellos.

3.1. El caso Snowden

Uno de los casos con mayor impacto Internacional es el de Edward Snowden quien sacó a la luz documentos del gobierno de EE.UU. y la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) en el año 2013. A partir de ese momento, se reveló la forma de vigilancia empleada por EE. UU. no sólo a sus ciudadanos, sino que tal nación recolectaba y analizaba información de cualquier persona en el mundo. El programa de vigilancia registró interesantes revelaciones como las de *WikiLeaks*, además que, la información se tornó de interés público con más de 1530 documentos publicados.

> En el año 2013, algunos periódicos sacaron a la luz información secreta de la NSA, la primera empresa en jaque fue *Verizon Communications Wireless*,[106] cuando le llegó una orden judicial para entregar todos los metadatos y con frecuencia diaria. Un día después, los mismos diarios revelan información de programas de espionaje secreto a nivel Internacional y es cuando sale a la luz el programa PRISM que es un *software* clandestino de vigilancia con la capacidad de recolectar masivamente las comunicaciones afectando a usuarios de empresas como Facebook, Apple, Google, por mencionar algunas[107].

Toda la información fue otorgada por Snowden a tres periodistas: Glenn Greenwald, Ewen MacAskill y Laura Poitras. La reunión fue en Hong Kong y el tema principal, espionaje realizado a comunicaciones digitales. ¿Cómo se obtuvo esa información? Se sabe que, Snowden era empleado de la empresa *Buzz Allen Hamilton* misma que era contratista de la NSA y gracias a eso podía acceder a información clasificada.

La veracidad de los documentos se puso en duda por el gobierno de EE. UU. y la declaración fue que Snowden traicionó la confianza de su propio país, revelando secretos, por lo que el entonces presidente Barack Obama declaró:

> No me gustan las filtraciones porque existe un motivo para que estos programas sean clasificados. Creo que el Sr. Snowden planteó algunas preocupaciones legítimas. El, cómo lo hizo fue algo que no siguió los procedimientos y prácticas de nuestra

[106]Empresa dedicada a la telefonía móvil, hasta hoy día es el mayor operador en Estados Unidos gracias a las fusiones realizadas con otros operadores.
[107]Obama explica por qué Estados Unidos no puede perdonar a Snowden. [En línea]. https://www.genbeta.com/actualidad/obama-explica-por-que-estados-unidos-no-puede-perdonar-a-snowden. [Página consultada el 09/VI/ 2019].

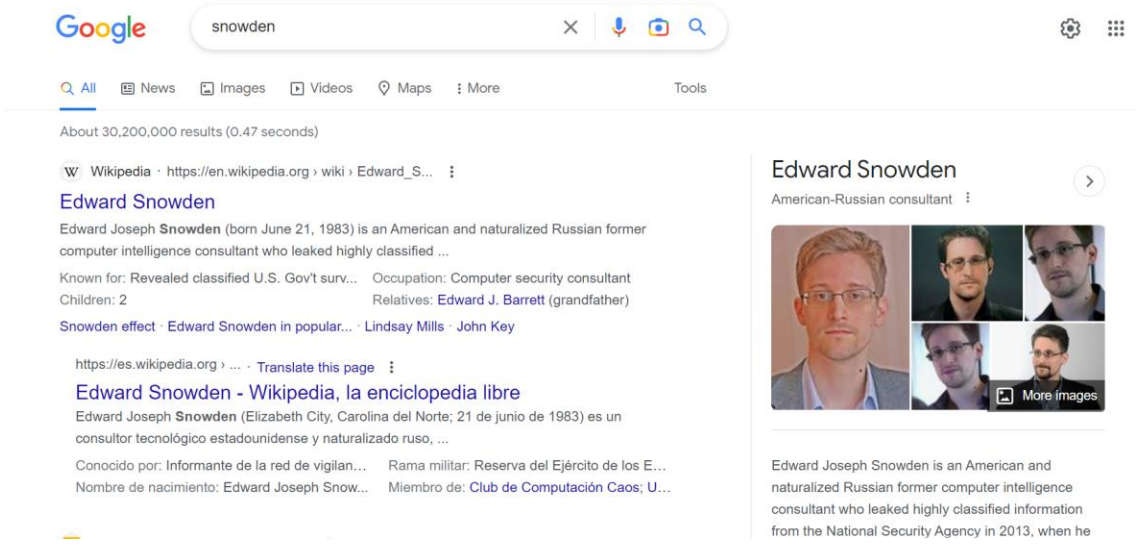
comunidad de inteligencia. Si todo el mundo tomase el camino de tomar sus propias decisiones sobre estos temas, entonces sería muy difícil tener un gobierno organizado o cualquier tipo de sistema de seguridad nacional[108].

Se sabe que los medios de comunicación que sacaron a la luz los documentos de Snowden fueron *The Guardian* de Inglaterra, The Washington Post de Estados Unidos, The New York Times de Estados Unidos, Propublica de Estados Unidos, *The Intercept* de Estados Unidos, Der Spiegel de Alemania, *L'Espresso* de Italia, O Globo de Brasil y Todo Noticias de Argentina. Adicionalmente se utilizaron otras fuentes que escribieron sobre los documentos de Snowden. Entre las más importantes se encuentra el portal Electrospaces.net y el libro El Imperio de la Vigilancia, escrito por Ignacio Ramonet que describe el contexto histórico de la NSA más allá de los documentos de Snowden[109].

A estas acciones de Snowden se le han sumado más personas con el objetivo de desmantelar el trabajo de vigilancia de los EE. UU. y, también, en muchos países se han realizado campañas para incitar a que se deje de realizar este tipo de acciones, a que se interrumpa el espionaje a la sociedad civil y a que las personas que hacen este tipo de trabajo lo suspendan.

Solamente para dar una idea del impacto del Caso Snowden, enseguida se muestran los resultados, cuando en el buscador de Google se pone la palabra Snowden. Obsérvese que, aparecen treinta millones doscientos mil ligas de posible consulta.

Figura 14. Resultado de búsqueda de la palabra Snowden en la web.



[108]La NSA, según las revelaciones de Snowden. [En línea]. http://www.rebelion.org/docs/234497.pdf. [Página consultada el 09/VI/ 2019].
[109] *Ibidem.*

Fuente: Snowden. [En línea]. https://www.google.com/search?q=snowden&rlz=1C1ALOY_esMX971MX971&oq=snowden&aqs=chrome.0.0i271j46i512l2j0i512l6j46i512.1501j0j15&sourceid=chrome&ie=UTF-8. [Página consultada el 09/ II/ 2022].

Entonces, lo que Snowden hizo, fue difundir información de un programa de vigilancia y debido a ello ahora es perseguido por su gobierno, arriesgándose a cumplir una sentencia mínima de 30 años. Gracias al refugio que le ofrece el gobierno de Rusia no ha podido ser extraditado a su país natal.

Interesante es reproducir algunas palabras de Glenn Greenwald sobre Snowden, a saber:

> A las dos de la tarde del domingo 9 de junio, hora oriental, el Guardián publicó el artículo que hacía pública la identidad de Snowden: «Edward Snowden: el delator de ilegalidades, divulgador de las revelaciones sobre vigilancia de la NSA». El artículo contaba la historia de Snowden, transmitía sus motivos y proclamaba que «pasará a la historia como uno de los reveladores de secretos más importante de Norteamérica, junto con Daniel Ellsberg y Bradley Manning». Se citaba un viejo comentario que Snowden nos había hecho a mí y a Laura: «Sé muy bien que pagaré por mis acciones… Me sentiré satisfecho si quedan al descubierto, siquiera por un instante, la federación de la ley secreta, la indulgencia sin igual y los irresistibles poderes ejecutivos que rigen el mundo que amo[110].

Así, se considera que Snowden, de ser un espía, pasó a ser el hombre más espiado del mundo. La siguiente tabla fue realizada con información tomada del sitio Hipertextual, destaca una interesante cronología de dicho personaje.

Tabla 7. Cronología del caso Snowden.

Año	Eventos
2006	Edward Snowden es contratado por la CIA, obteniendo acceso a información confidencial de alto secreto.
2007 - 2009	Snowden es enviado a Génova, Suiza como experto en ciberseguridad de la CIA. Durante este periodo, según confirmó posteriormente al diario The Guardian, comenzó a sentirse

[110]Glenn Greenwald. *Sin un lugar donde esconderse.* [En línea]. https://reexistencia.files.wordpress.com/2011/02/snowden-completo.pdf [Página consultada el 08/VII/2019].

	desilusionado de cómo su gobierno controlaba la información del resto del mundo.
2009 – marzo 2012	El supervisor de Snowden envía un informe negativo sobre su comportamiento y hábitos de trabajo, afirmando que Snowden intentó acceder a archivos clasificados a los que no tenía autorización. Poco después, Snowden abandona la CIA y comienza a trabajar para la NSA en Hawaii.
Diciembre 2012 – enero 2013	Snowden contacta con personas como Glenn Greenwald, abogada y columnista y columnista del diario The Guardian.
Mayo 2013	Snowden comienza a enviar documentos a periodistas de The Guardian y del Washington Post. A finales de ese mismo Snowden mes viaja a Hong Kong, donde posteriormente viajarán los periodistas contactados previamente.
Junio 5, 2013	Los primeros documentos proporcionados por Snowden son publicados en el diario The Guardian. El título es clasificador: "La NSA recolecta registro de llamadas telefónicas de millones de consumidores de Verizon".
Junio 6, 2013	The Guardian y el Washington Post publican un artículo sobre PRISM, el programa de la NSA que obligue a las grandes compañías del sector tecnológico a ceder los datos de sus usuarios a las autoridades de los Estados Unidos mediante puertas traseras.
Junio 11, 2013	El diario The Guardian revela a Snowden como el filtrador de todas las informaciones publicadas. Snowden s inmediatamente despedido de Bozz Allen Hamilton, una de las empresas subcontratadas por la NSA y en la que Snowden trabajaba.
Junio 13, 2013	Snowden afirmar que los Estados Unidos han hackeado y espiado sistemas chinos durante años. Posteriormente, también se confirmará espionaje a sistemas rusos.
Junio 14, 2013	El Departamento de Justicia de los Estados Unidos toma acciones. Snowden recibe cargos por transmitir comunicaciones e informaciones de carácter confidencial asociados a los servicios de inteligencia de los Estados Unidos.
Junio 16, 2013	Los servicios de inteligencia británicos y estadounidenses recolectaron información de políticos asistentes a las cumbres del G8, G20 y las Naciones Unidas.
Junio 21, 2013	The Washington Post revela que la NSA recolecta más de 250 millones de bandejas de correo electrónico y listas de contactos de servicios como Yahoo, Gmail o Facebook.
Junio 23, 2013	Snowden abandona Hong Kong y viaja hasta Ecuador, con una parada prevista en el aeropuerto de Rusia. Las autoridades estadounidenses rescinden su pasaporte y queda encerrado en Rusia.
Junio 30, 2013	The Guardian revela programas de espionaje de la NSA dirigidos a embajadas de países extranjeros.
Agosto 1º, 2013	Snowden consigue asilo político temporal en Rusia.

Agosto 29, 2013	The Washington Post asegura pagos a compañías estadounidenses de telecomunicación a cambio de acceso ilimitado a sus infraestructuras.
Agosto 2013 – enero 2014	Numerosas informaciones revelan el espionaje de la NSA a gobiernos extranjeros, empresas multinacionales, medios de comunicación y entidades bancarias. Se incluye a España, Italia, Venezuela, Colombia, etc.
Enero 2, 2014	El New York Times afirma que la NSA ya trabaja en un ordenador cuántico capaz de descifrar cualquier tipo de encriptación, abriendo el abanico de posibilidades de los servicios de inteligencia estadounidenses.
Enero 17, 2014	La NSA asegura que los ciudadanos estadounidenses no están viendo su privacidad violada.
Enero 27, 2014	NBC News afirmar que los servicios de inteligencia estadounidenses y británicos logró un *software* capaz de monitorizar You Tube en tiempo real, recolectando direcciones, vídeos visualizados, etc.
Febrero 7, 2014	NBC News afirmar que los servicios de inteligencia británicos usaron técnicas ilegales contra otras naciones, grupos terroristas, periodistas, diplomáticos,
Febrero 27, 2014	Los servicios de inteligencia británicos interceptaron y recolectaron imágenes procedentes de webcams, datos que fueron compartidos con las bases de datos de la NSA.
Mayo 13, 2014	Se informa que la NSA interceptaba físicamente los routers, servidores y sistemas de comunicación antes de ser exportados de los Estados Unidos.
Febrero 23, 2015	Snowden realiza una conferencia en conjunto con los periodistas que iniciaron las publicaciones sobre PRISM y NSA.
Septiembre 29, 2015	Snowden inaugura una cuenta de Twitter mediante la cual se comunicará públicamente.
Octubre 30, 2015	El Parlamento Europeo celebra una votación en l que se absuelve a Snowden de todos los cargos en los diferentes países de la Unión Europea.
Marzo 13, 2016	Snowden es entrevistado por la cadena televisiva española Sexta. Aquí explica los métodos utilizados por el gobierno estadounidense y su visión sobre el futuro de la privacidad.

Fuente: Hipertextual. *Cronología del caso Snowden, el hombre más buscado del mundo*. [En línea]. https://hipertextual.com/2016/03/cronologia-edward-snowden [Página consultada el 08/VII/ 2019].

A la fecha, se supone que Snowden está asilado en Rusia, sin que se sepa prácticamente nada sobre él, debido a su vida discreta y alejada de los focos.

3.2. La Operación Aurora

La Operación Aurora, también conocida como Comele o Hydraq consistió en:

> Las infiltraciones de atacantes chinos lograron infiltrarse en una base de datos de los sistemas de Google y tuvieron acceso datos confidenciales sobre objetivos de vigilancia

estadounidenses. La Operación Aurora estuvo dirigida al menos a 34 empresas, entre ellas Google, Adobe, Juniper, Rackspace, Symantec, Northrop Grumman, Morgan Stanley y Yahoo!. Se sabe que el nombre Operación Aurora fue dado por los investigadores luego de detectar en el código fuente de uno de los *malware* involucrados en el ataque, cadenas de caracteres que se refieren al proyecto como "aurora"[111].

La manera más sencilla de explicar el funcionamiento de este *malware* es que cualquier día puedes encontrar mails misteriosos en la bandeja de entrada de tu correo personal o empresarial, este correo te hace una invitación a visitar un sitio que seguramente no es conocido. Al dar clic al link, da inicio a uno de los ataques cibernéticos más sofisticados de nuestra era, la bien llamada "Operación Aurora" el cuál tiene como objetivo el robo de información personal o empresarial y que puede suceder en unos cuantos minutos.

De acuerdo con Mieres, en cuanto al objetivo de esta operación, existen un par de hipótesis:

- "Que el ataque fue motivado con el ánimo de robar información de propiedad intelectual a grandes compañías.
- Que su objetivo principal fue la intención de robar cuentas de Gmail de un activista de derechos humanos en China y, aunque el ataque fue hecho público por Google durante la segunda semana de enero de 2010, pero, aparentemente comenzó a gestarse desde diciembre del 2009" [112].

Como podemos observar, "la vulnerabilidad es tan delicada, que se puede decir que lo grave es que este tipo de ataques son muy fáciles de explotar cuando no se dan todas las condiciones necesarias de seguridad, ya que con el solo hecho de acceder a *Internet* a través de un navegador o abrir un correo electrónico y, si encuentra la vulnerabilidad, el atacante podrá acceder a información confidencial de la organización".[113]

Actualmente, este *malware* es uno de los más resistentes y peligrosos para las compañías, gobiernos, instituciones e incluso como sociedad, se tienen que datos que en los últimos 12 meses se han incrementado los casos de robo de información mediante este tipo de ataque, actualmente, las regulaciones en torno a los ataques cibernéticos han sido un tema de prioridad ya que es imperativo que las organizaciones estén preparadas para más ataques y para la inestabilidad general que pueda representar.

---

[111]*Noticias sobre seguridad de la información. Operación Aurora, exfiltró información de espionaje desde Googl*e. [En línea]. https://blog.segu-info.com.ar/2013/05/operacion-aurora-exfiltro-informacion.html. [Página consultada el 14/VII/2019].

[112]*¿Qué es operación Aurora*? [En línea]. https://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/. Página consultada el 14/VII/2019].

[113]Operación Aurora. El ataque hacker mejor planeado de los tiempos. [En línea]. https://si3h-c5ir7.blogspot.com/2011/09/operacion-aurora-el-ataque-hacker-mejor.html. [Página consultada el 14/VII/2019].

3.3. El Caso Echelon

La Red Echelon como es mundialmente conocida, fue creada por Estados Unidos y Reino Unidos durante la Segunda Guerra Mundial, su objetivo principal era interceptar las comunicaciones de los nazis y así tener una ventaja sobre el enemigo. Se sabe que, “Echelon tuvo como objetivo original "vigilar" a los gobiernos del llamado bloque socialista y a los movimientos internacionales considerados "subversivos" por los gobiernos participantes en el sistema”.[114]

A pesar de que en un inicio solo se mantenía con los países ya mencionados, en la década de los 50´s creció su radio de acción y se anexaron Canadá, Australia y Nueva Zelanda, durante esta época, su objetivo era controlar las comunicaciones en la guerra fría.

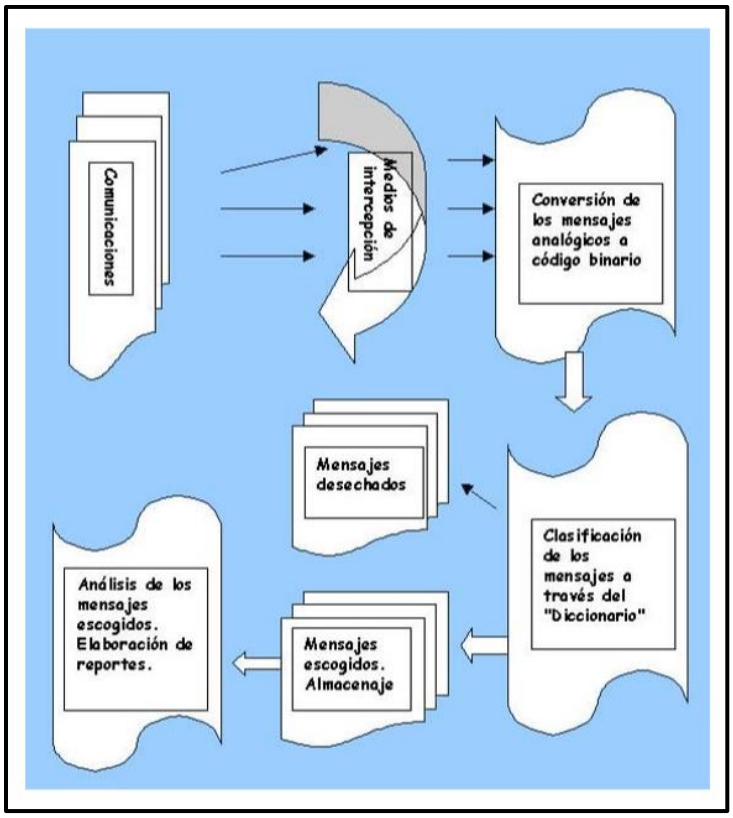
Ornelas explica que en la red Echelon:

> Se sitúan todas las formas de comunicación privada: llamadas telefónicas, faxes, señales de radio, correos electrónicos y télex, entre las más comunes, constituyendo la materia más sencilla de espiar por el sistema.
>
> Respecto al funcionamiento, el autor comenta que la primera capa de ECHELON consiste en los medios de intercepción que captan las comunicaciones y las transmiten a los centros de tratamiento. Centralmente, ello comprende: las estaciones terrestres, los navíos (barcos y submarinos) espías y los satélites secretos ubicados a gran altura (mayor que la de los satélites civiles). El espionaje en *Internet* se realiza a través de las dorsales, la mayoría de las cuales está manejada por empresas o instituciones estadounidenses. En cuanto a las capacidades de decriptaje, ECHELON está a la vanguardia. Se dice que el sistema ya logró "romper" el algoritmo de criptaje 2028-bits, que es la "llave de protección" más utilizada por las computadoras[115].

A continuación, se comparte una infografía también realizada por el autor Ornelas donde precisa el funcionamiento de esta red.

[114]Raúl Ornelas Bernal. *Un mundo nos espía. El escándalo Echelon*. [En línea]. http://let.iiec.unam.mx/sites/let.iiec.unam.mx/files/OrnelasEchelonChiapas9.pdf. [Página consultada el 15/VII/2019].
[115]*Ibidem.*

Figura 15. Primera capa de ECHELON.



Fuente: Raúl Ornelas Bernal. *Un mundo nos espía. El escándalo Echelon*. [En línea]. http://let.iiec.unam.mx/sites/let.iiec.unam.mx/files/OrnelasEchelonChiapas9.pdf. [Página consultada el 15/VII/2019].

"Respecto al funcionamiento de ECHELON, considérese lo siguiente:

- El sistema de espionaje se basa en la escucha de las comunicaciones por medio de *sniffers* y su posterior filtrado.
- Este filtrado se centra en la identificación de palabras clave previamente fijadas en inmensos diccionarios. Estas palabras pueden pertenecer tanto a textos como a voces reales y ser pronunciadas y/o escritas en varios idiomas (inglés, castellano, francés, árabe, chino, japonés...)
- El sistema informático posee por lo tanto potentes *olfateadores* y programas de reconocimiento de voz. Se habla de que puede filtrar 2.000 millones de mensajes en una hora.
- Tal y como está organizada la red, ésta no permite, por ejemplo, a las autoridades neozelandesas conocer los diccionarios usados por USA y Gran Bretaña, si bien lo contrario sí es posible. Aquí se demuestra de nuevo el talante discriminatorio de los Estados Unidos y Gran Bretaña.

Primeramente, se definen las palabras clave, como por ejemplo *bomba, Busch, atentado, droga, Sadam Hussein, Castro*, siempre definidas en varios idiomas. Se pasa entonces a olfatear las comunicaciones mundiales. Se habla de un poder de captación del 90% de las mismas, si bien se cree que este porcentaje solo afecta a las comunicaciones de *internet*.

- Teniendo en cuenta que casi todas las comunicaciones vía *internet* mundiales, independientemente de dónde se produzcan, pasan por nodos de comunicación de los Estados Unidos y por nueve puntos de control de la NSA. Es decir, que ni siquiera tiene que ir a buscarlas, las traen hasta la cocina. Una vez que se detecta una comunicación conteniendo o bien palabras clave o bien ciertas combinaciones de ellas (por ejemplo, "bomba", "gobierno" y "atentado" en el mismo mensaje), el sistema informático pasa a monitorearla y grabarla. Esta comunicación será entonces etiquetada y enviada a distintos centros de análisis.
- Dependiendo del origen y fecha de la comunicación será marcada con un número clave. Se transcribe, descifra, traduce y se guarda entonces como un informe. Estos informes recibirán un código dependiendo del grado de secretismo otorgado al mismo: "*Morai*" equivale a secreto. Después le siguen los códigos "*Spoke*" (más secreto), "*Umbra*"(alto secreto), "*Gamma*" (comunicaciones rusas) o "*Druid*" (destinado a países no miembros de la red)" [116].

Unas de las más importantes estaciones de rastreo y escucha de ECHELON se sitúan en:

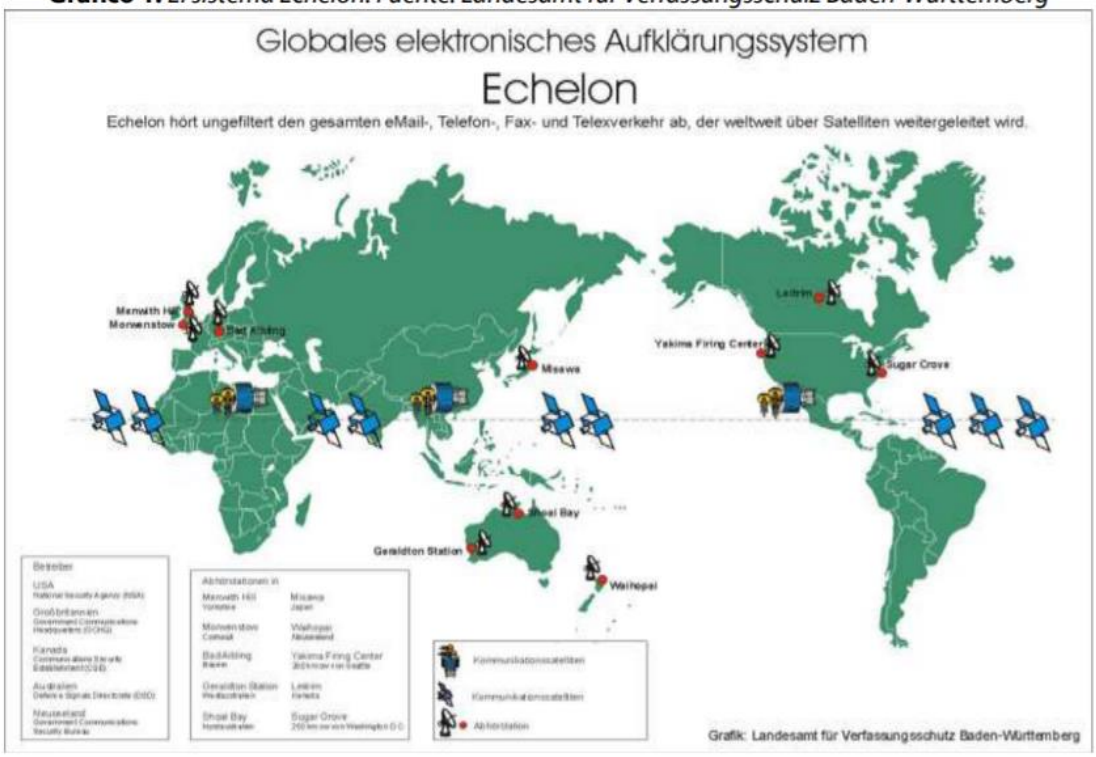
- Sugar Grove, Virginia, USA.
- Leitrim, Canadá.
- Sabana Seca, Puerto Rico, estado asociado de USA.
- Menwith Hill, Gran Bretaña.
- Bad Aibling, Base norteamericana en Alemania.
- Waihopai, Nueva Zelanda.
- Shoal Bay, Australia.[117]

Sin embargo, mantiene bases en todo el mundo, a continuación, el mapa de ellas.

[116]La Red Echelon: la gran oreja. [En línea]. https://www.bibliotecapleyades.net/ciencia/echelon02.htm [Página consultada el 15/VII/2019].
[117] *Ibidem.*

Figura 16. Mapa de las bases globales de Echelon.

Gráfico 1: *El sistema Echelon. Fuente: Landesamt für Verfassungsschulz Baden-Württemberg*



Fuente: La Red Echelon: la gran oreja. [En línea]. https://www.bibliotecapleyades.net/ciencia/echelon02.htm [Página consultada el 15/VII/2019].

Después de mantener en secreto por muchos años la información de Echelon, en el mes de septiembre del año 2001, el Parlamento Europeo, denunciaba la existencia de una red de espionaje con dimensión planetaria. Este sistema, "se ha utilizado con fines militares, pero también económicos e incluso privados, llegando a vulnerar el derecho fundamental a la intimidad de la sociedad en nombre de la lucha contra el terrorismo"[118]. Al respecto, se realizó una declaración:

> La mayor aureola de secreto envuelve las sofisticadas labores de espionaje conocidas como el sistema ECHELON. Por primera vez, el lector en lengua española tiene en sus manos un informe fidedigno, avalado por el Parlamento europeo, en el que se detallan las turbias actividades de los servicios de inteligencia anglosajones -EE.UU., Reino Unido, Canadá, Australia y Nueva Zelanda- en su empeño por

[118] *Echelon. La red de espionaje planetario*. [En línea]. http://www.melusina.com/rcs_gene/0068-e_echelon.pdf [Página consultada el 18/VII/2019].

controlar las comunicaciones mundiales. La devastadora conclusión del informe es que nadie está a salvo de la mirada de ECHELON...[119].

3.4. El Caso Cambridge Analityca

"Cambrige Analytica es una firma privada de comunicación estratégica y análisis de información vinculada al Partido Republicano de Estados Unidos y con oficinas en Nueva York, Washington y Londres"[120].

El caso de Cambrige Analytica ha traído una serie de circunstancias internacionales que pusieron en riesgo la información de la sociedad, según el blog de celag.org, *Cambridge Analytica* es una empresa proveniente de Londres que nación en el año 2013, su fundador fue Alexander Nix.

Dicha empresa, se dedica al uso "al uso de datos para cambiar el comportamiento de audiencias y sus análisis y estudios son vendidos a empresas y también a políticos. Han trabajado en más de cien campañas políticas en el mundo, y en América Latina han trabajado en Argentina, Brasil, Colombia y México"[121].

El punto clave en el que se dio a conocer a esta empresa a nivel internacional fue en el momento en el que obtuvo información de alrededor de 50 millones de usuario y que cabe aclarar, no fue obra de la empresa como tal, sino que este hecho ha sido atribuido

> "Al profesor de la Universidad de Cambridge Aleksander Kogan, el cual, como un proyecto personal, desarrolló en 2013 un test de personalidad en formato de aplicación de Facebook. Unos 265.000 usuarios completaron el test que requería permiso para acceder a información personal y de la red de amigos, sin el consentimiento de estos últimos. Fue así como Kogan se hizo de actualizaciones de estado, "me gusta" y hasta mensajes privados de más del 15% de la población de EE.UU., los cuales luego vendió a la empresa de Nix para dirigir el resultado de las elecciones en Estados Unidos y hacer ganar a Donald Trump."[122].
>
> *Cambridge Analytica* logró saber cuál debía ser el contenido, tema y tono de un mensaje para cambiar la forma de pensar de los votantes de forma casi individualizada. Pero la compañía no solo envió publicidad personalizada, sino que

[119] *Ibidem.*
[120] *¿Cambridge Analytica* opera en México? Esto es lo que se sabe. [En línea]. https://politica.expansion.mx/mexico/2018/03/21/cambridge-analytica-opero-en-mexico-esto-es-lo-que-se-sabe. [Página consultada el 17/VII/2019].
[121] Celag.org. *"Cambridge Analytica, Big Data y su influencia en las elecciones"* [En línea]. https://www.celag.org/cambridge-analytica-el-big-data-y-su-influencia-en-las-elecciones/. 43472797 [Página consultada el 17/VII/2019].
[122] *Ibidem.*

> desarrolló noticias falsas que luego replicó a través de redes sociales, blogs y medios[123].

Según las investigaciones, tiempo después uno de los creadores de este sistema para recaudar datos de Facebook, confesó a "*The Observer*" que, gracias al sistema de la misma aplicación, lograron almacenar millones de perfiles de usuarios para después crear modelos digitales para tener múltiples áreas de oportunidad en las elecciones.

Por otro lado, se sabe que, "tanto *Cambridge Analytica* como *Facebook* han sido sujetos de investigación por parte de la Comisión Británica de Información y parte de la Comisión Electoral del Reino Unido, que analizan si la empresa consultora tuvo injerencia en el referéndum de junio de 2016 para decidir la salida británica de la Unión Europea"[124].

Parte determinante en este caso fue la declaración de Mark Zuckerberg ante el Congreso de los Estados Unidos:

> Al inicio de la audiencia, el senador Frank Pallone hizo una pregunta difícil. Le preguntó a Mark por qué la red social no puso por defecto la configuración de privacidad para que la gente pudiera; en un inicio, decidir si quiere o no compartir sus datos con la empresa. Por el momento, la opción es al revés: inicias compartiendo sin saberlo, pero puedes decidir no hacerlo más adelante. La idea era que el CEO de Facebook respondiera con sí o no a la siguiente cuestión: ¿Estaría dispuesto a que la configuración inicial de Facebook por default sea no compartir datos; a menos de que la gente la cambie para compartirlos? Mark no pudo responder "Senador, es un tema difícil que merece una respuesta más amplia que una sola palabra". "Eso es decepcionante para mí", respondió el senador[125].

Sin embargo, en sus declaraciones, Zuckerberg dijo: "No tuvimos una visión lo suficientemente amplia de nuestra responsabilidad, y ese fue un gran error. Fue un error mío y lo siento".[126]

Como ya se mencionó, el tema de carácter internacional ha cruzado todas las fronteras, hay registros sobre la presencia de *Cambridge Analytica* en México, sobre esto se sabe que las operaciones en nuestro país comenzaron con la instalación en el año 2016, y no es sino hasta 2017, cuando la agencia de noticias *Bloomberg* reveló que

---

[123] BBC News. *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día.* [En línea]. https://www.bbc.com/mundo/noticias-43472797 [Página consultada el 18/VII/2019].

[124]Proceso. Cambridge Analytica: el poder de la desinformación. [En línea]. https://www.proceso.com.mx/527974/cambridge-analytica-el-poder-de-la-desinformacion [Página consultada el 19/VII/2019].

[125] Fayer Wayer. *Segundo día: puntos clave sobre la declaración de Mark Zuckerberg ante el Congreso*. [En línea]. https://www.fayerwayer.com/2018/04/segundo-dia-puntos-clave-zuckerberg/ [Página consultada el 09/VII/2019].

[126] *Ibid.*

representantes de la empresa estaban ofreciendo sus servicios con vistas a las elecciones mexicanas de julio de este año.

Así, "Brittany Kaiser, ex directora de *Cambridge Analytica*, aceptó la captura de datos personales en México desde una aplicación. Sin embargo, negó que su utilización fuera para fines políticos"[127]. Se calcula que, aproximadamente 1.2 millones de usuarios entre México y Colombia utilizaron la aplicación (Pig.gi) que capturó los datos, de acuerdo con datos de *Cambridge Analytica*.

Los datos sobre el uso de esta aplicación están relacionados directamente con los partidos políticos Partido Revolucionario Institucional y Partido Acción Nacional, sin embargo, candidatos presidenciales, negaron en su momento el uso de este *software* para generar posicionamiento digital durante las campañas políticas incluso uno de los candidatos comentó: "Si Facebook está operando en el país debe sujetarse a las leyes mexicanas. Sí es un problema si Facebook no revela quiénes están comprando las pautas, si lo pueden hacer cuánto costaron y para qué candidato y qué campaña, entonces vamos a tener un problema gravísimo"[128]

Considérese que, la consultora política británica Cambridge Analytica, dio a conocer el cierre oficial de sus puertas el 2 de mayo de 2018 debido a la insolvencia provocada por la noticia, los resultados son los siguientes:

- "Estados Unidos es el país con el mayor número de afectados con 70,632,350 personas, seguido de Filipinas con 1,175,870 usuarios y en tercero Indonesia con 1,096,666
- México ocupa el quinto lugar con 789,880 usuarios afectados, lo cual representa 0.9% del total de 87 millones de personas impactadas por el caso.
- Facebook, actualizó la cifra a 87 millones"[129].

Durante todo el caso de *Cambridge Analytica*, las acciones de *Facebook* cayeron aproximadamente un 7%, el Parlamento Británico ha llamado al fundador de la red social a

[127]Forbes. *Cambridge Analytica sí capturó datos personales en México: exdirectora*. [En línea]. https://www.forbes.com.mx/cambridge-analytica-si-capturo-datos-personales-en-mexico-ex-directora/ [Página consultada el 09/VII/2019].
[128] *¿Cambridge Analytica* opera en México? Esto es lo que se sabe. [En línea]. https://politica.expansion.mx/mexico/2018/03/21/cambridge-analytica-opero-en-mexico-esto-es-lo-que-se-sabe. [Página consultada el 17/VII/2019].
[129]Expansión. "*Casi un millón de mexicanos afectados por Cambridge Analytica".* [En línea]. https://expansion.mx/tecnologia/2018/04/04/casi-un-millon-de-mexicanos-afectados-por-cambridge-analytica. [Página consultada el 18/VII/2019].

comparecer ante las acusaciones, *Cambridge Analytica*, por su parte, aseguró que cuando supo cómo Kogan había recopilado los datos, los borró.

"Mientras tanto en México, el Senado señaló que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) inició una investigación de oficio con el propósito de corroborar el cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares por parte de las empresas que pudieran estar involucradas en los hechos relacionados con el caso "*Cambridge Analytica*", señalada de haber obtenido información de 87 millones de usuarios de Facebook, para fines electorales".[130]

3.5. Casos mexicanos de espionaje

En México se ha visto un creciente desarrollo de casos en contra de la sociedad civil, actualmente la Secretaría de la Función Pública tiene procesos abiertos del tipo digital, ya que es el "organismo encargado de realizar las investigaciones tachadas como espionaje al gobierno. La dependencia gubernamental, es la encargada de realizar auditorías al gobierno digital, así como vigilar que los servidores públicos federales se apeguen a la legalidad durante el ejercicio de sus funciones, sanciona a los que no lo hacen así".[131]

"En nuestro país, las autoridades –siempre que cuenten con una autorización judicial– son las únicas facultadas para realizar actos de espionaje. Cualquier otra persona que realice este tipo de prácticas indudablemente está violando todo el régimen legal mexicano e incurriendo en la comisión de un delito"[132].

A continuación, se presentan casos de vigilancia a la sociedad que han repuntado en los últimos años en México, mismos que hasta hoy día, es una práctica muy eficiente a aquellos sujetos que buscan vulnerar y que de una u otra forma, tiene repercusiones en los Derechos Humanos ya sea en la persona o institución en la que se enfocan y/o centra la vigilancia a través de los mismos.

---

[130] Gaceta del Senado. [En línea]. https://www.senado.gob.mx/64/gaceta_del_senado/documento/81027. [Página consultada el 09/ XI/ 2019].

[131] Secretaría de la Función Pública. [En línea]. http://pcop.funcionpublica.gob.mx/index.php/conoce-la-sfp.html. [Página consultada el 09/ XII/ 2019].

[132] Deloitte. *"Sin autorización judicial, espiar es un acto ilegal".* [En línea]. https://www2.deloitte.com/mx/es/pages/dnoticias/articles/actividades-de-espionaje.html. [Página consultada el 09/ XII/ 2019].

Si bien, los DD.HH. son un punto importante en el proceso de creación y uso de estos software, el capítulo se encuentra enfocado en como han sido utilizados, en quién y ejemplos de los mismos siendo vigilados bajo el foco del camino de la investigación.

3.5.1. El *software Pegasus*

La empresa que desarrolló este *software* es *NSO Group,* una compañía israelí que se dedica a vender herramientas de vigilancia. *Pegasus* es tecnología utilizada principalmente para la vigilancia de terroristas y criminales, sin embargo, ha sido vendida a gobiernos para la vigilancia de sus ciudadanos, convirtiéndose en una peligrosa herramienta de espionaje en dispositivos informáticos,

Actualmente, estas herramientas de vigilancia no son utilizadas contra el objetivo inicial, sino contra la sociedad, dañando los derechos humanos. La herramienta funciona de una forma muy sencilla, la persona a la que se busca afectar recibe un mensaje de texto junto con un enlace o nota periodística, al hacer clic en el enlace, lo redirige a un sitio al tiempo que instala el *malware* en el dispositivo lo que facilita el rápido acceso a todas las aplicaciones en el equipo, por ejemplo: contactos, mensajes y/ correos y también permite activar el micrófono y la cámara.

En el caso de México, esta herramienta fue adquirida durante el gobierno de Enrique Peña Nieto y fue en nuestro país donde se registraron más dominios utilizados, a saber: "Unonoticias.net, youtube.com.mx, fb-accounts.com y whatsapp-app.com, ninguno de estos pertenece al sitio oficial de las redes o aplicaciones"[133].

Se sabe que: "El primer registro de esto fue en 2015 al periodista Rafael Cabrera, quien contó a través de Twitter sobre los mensajes que le habían llegado a su móvil, no todo terminó ahí, los casos continuaron con dos activistas y un científico que se promulgaron en contra de las bebidas azucaradas[134].

Citizen Lab, Artículo 19 y R3D (Red de Defensa de los Derechos Digitales) han seguido muy de cerca el caso en México, incluso han realizado artículos completos sobre el tema. *Citizen Lab* encontró que hasta 2018 el *software* seguía operando en México a través de suplantar conocidos medios como Uno TV, Uno noticias y Animal Político. "Según

[133] *Pegasus, el mayor spyware de móviles, ha infectado a Iphone y Android en 45 países*. [En línea]. https://www.adslzone.net/2018/09/18/*Pegasus*-spyware-nso-group/. [Página consultada el 09/ XI/ 2018].

[134] *¿Qué es Pegasus? el malware usado para espiar a México*. [En línea]. http://www.milenio.com/estilo/que-es-*Pegasus*-el-*malware*-usado-para-espiar-en-mexico. [Página consultada el 09/ XI/ 2018]

el New York Times, el acceso a un caso exitoso de *Pegasus* cuesta alrededor de un millón cuatrocientos mil pesos M.N."[135] .

Si bien no existe una regulación que impida este tipo de actos, tampoco hay uno que sí lo haga, por lo hasta hoy en día, sin duda alguna, se juega con el discurso de la seguridad nacional, a pesar de ser utilizado contra la sociedad civil y lo costoso que puede llegar a ser. Cabe señalar que: "Entre 2016 y 2018, *Citizen Lab* detectó 1,091 direcciones IP y 1,014 dominios que coinciden con la infraestructura de *NSO Group*, la empresa de origen israelí que diseñó el *software*[136]".

Citizen Lab ha confirmado que la herramienta *Pegasus* sigue siendo utilizada para actividades de vigilancia en México. El reporte señala que, la misma vigilancia va en contra de la sociedad mientras que *NSO Group* se respalda en que su *software* sólo tiene licencia en países con Marco de Ética de Negocios. Entre los más diversos personajes y empresas afectadas y vigiladas por *Pegasus*, están los siguientes:

> Mario Patrón, Stephanie Brewer y Santiago Aguirre de la Organización de Derechos Humanos Centro Miguel Agustín Pro Juárez, (Centro Prodh); Carmen Aristegui, Rafael Cabrera y Sebastián Barragán del Portal de Noticias (Aristegui Noticias), así como Emilio Aristegui, hijo de la periodista Carmen Aristegui; el periodista Carlos Loret de Mola; Juan Pardinas y Alexandra Zapata del Instituto Mexicano por la Competitividad (IMCO); y Daniel Lizárraga y Salvador Camarena de la organización Mexicanos Contra la Corrupción y la Impunidad (MCCI)[137].

---

[135] *Ibid.*

[136] *Detectan en México tres operadores activos del software espía Pegasus*. [En línea]. https://aristeguinoticias.com/2009/mexico/detectan-en-mexico-tres-operadores-activos-del-*software*-espia-*Pegasus*/. [Página consultada el 09/XI/ 2018].

[137] Gobierno Espía: La vigilancia sistemática en contra de los periodistas y defensores de Derechos Humanos en México. [En línea]. https://imco.org.mx/wp-content/uploads/2017/06/Comunicado_Orgs.pd. [Página consultada el 20/VII/ 2019].

Figura 17. Imagen de promoción de la herramienta *Pegasus*.

Fuente: *Pegasus* la impresionante herramienta de espionaje se utilizó contra un periodista en México. [En línea]. https://www.xataka.com.mx/otros-1/*Pegasus*-la-impresionante-herramienta-de-espionaje-se-utilizo-contra-un-periodista-en-mexico. [Página consultada el 20/VII/2019].

Por último, considérese que, a pesar de que las autoridades están obligadas a realizar y esclarecer la investigación del uso de espionaje contra la sociedad civil, no se han dado avances o explicación alguna del uso de la información que obtuvieron ni de lo que sucederá con esta situación de vigilancia por parte del gobierno. Muchas personas y sociedades se han sumado para que esto deje de pasar, hasta hoy día la lista sigue incrementando su número de inconformidades, denuncias y agresiones sin repercusiones legales sobre el Estado o precursores de esta nueva tecnología contra los derechos humanos y la sociedad civil.

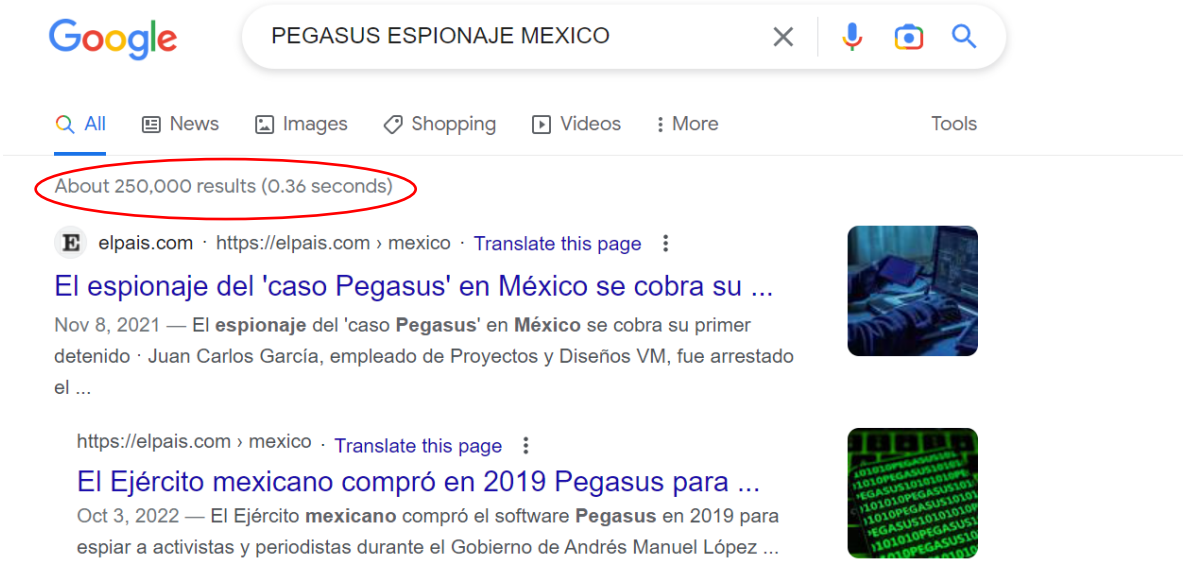
Para concluir este apartado, reproduzcamos el pensamiento de Juan Pardinas, a saber:

> Nuestro diseño institucional en procuración de justicia es un crimen contra la lógica y va en contra del sentido común. México necesita una Fiscalía y ministerios públicos autónomos, para investigar casos como el de *Pegasus*, en los que la propia estructura del Estado se convierte en parte acusada… la resolución de un Juez en la que se ordena a la PGR admitir las pruebas aportadas por la defensa de las víctimas de espionaje, es una acción bienvenida…sin embargo, considero que es una escena del

surrealismo mexicano, ya que la parte acusada es una de las instituciones que está a cargo de la investigación[138].

De la misma manera en que se ha estado mostrando, al colocar las palabras *PEGASUS* ESPIONAJE MÉXICO aparecen 250,000 resultados a consultar:

Figura 18. Imagen de búsqueda de la palabra *Pegasus* tomada de Google México



Fuente: *Pegasus* espionaje México. [En línea]. https://bit.ly/3IuD47i [Página consultada el 09/II/2022].

3.5.2. Aristegui y la Casa Blanca

"En un reporte publicado por las organizaciones Article19, R3D y SOCIAL TIC se revela una serie de ataques contra periodistas y activistas en México, ocurridos entre enero de 2015 y julio de 2016, mediante el *malware Pegasus*"[139]. De esta manera:

> El 24 de agosto de 2016, los investigadores del Citizen Lab de la Universidad de Toronto documentaron el método de infección del *malware Pegasus* gracias al activista Ahmed Mansoor, defensor de derechos humanos radicado en los Emiratos Árabes Unidos. En términos generales, el modus operandi de la infección consiste en el envío de un mensaje SMS al objetivo con un texto que busca engañarlo, mediante el uso de técnicas de ingeniería social4, para hacer clic en un enlace adjunto. Al hacer

[138]Casos como *Pegasus* demuestran necesidad de tener MPS y Fiscalía Autónomos: Pardinas. [En línea]. https://aristeguinoticias.com/2905/mexico/casos-como-*Pegasus*-demuestran-necesidad-de-tener-mps-y-fiscalia-autonomos-pardinas/. [Página consultada el 20/VII/2019].

[139] 2017 Jun 18 GOBIERNO ESPÍA. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. [En línea]. http://inep.org/content/view/479/106/. [Página consultada el 14/I/2020].

clic en el enlace, el navegador se abre y redirige al objetivo a uno de los sitios web de la infraestructura de NSO Group, dándole la oportunidad al *malware* de instalarse en el dispositivo gracias a una vulnerabilidad en el sistema operativo. De este modo, el atacante gana acceso a los archivos guardados en el equipo, así como a los contactos, mensajes y correos electrónicos. El *malware* también obtiene permisos para usar, sin que el objetivo lo sepa, el micrófono y la cámara del dispositivo. Según reportes de The New York Times, cada infección exitosa tendría un costo que oscila alrededor de los $77,000.00 USD[140].

Ahora, el 9 de noviembre de 2014, Carmen Aristegui en conjunto con otros periodistas publicaron el reportaje:

> "La casa blanca de Enrique Peña Nieto" en el portal Aristegui Noticias, así como en varios medios impresos nacionales e internacionales. El reportaje denunció que "la propiedad, ubicada en el número 150 de la calle Sierra Gorda y tasada en siete millones de dólares, estaba a nombre del contratista Juan Armando Hinojosa Cantú, beneficiado con importantes contratos durante la administración de Enrique Peña Nieto como gobernador del Estado de México y, posteriormente, como presidente"[141].

Hay que tomar en cuenta que:

> Los periodistas que realizaron el reportaje de la casa blanca formaban parte, al momento de la publicación, de la Unidad de Investigaciones Especiales de MVS Noticias Primera Emisión. La investigación salió en Aristegui Noticias y otros medios debido a que los concesionarios solicitaron a Carmen Aristegui (entonces titular del espacio radiofónico Primera Emisión) no publicar el reportaje en MVS. Meses más tarde, en marzo de 2015, el equipo fue despedido, en lo que la periodista calificó70 como "una errática, torpe y artificial escalada con el propósito evidente de silenciar entero el programa de noticias[142].

Cabe señalar que, el registro de agresiones y mensajes en contra de Aristegui y su equipo de trabajo además de su hijo es largo, como lo señala la siguiente tabla plasmada en la investigación de Article19, R3D y SOCIAL TIC.

---

[140] Article19, R3D y SOCIAL TIC. Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. [En línea]. https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf. [Página consultada el 14/I/2020].

[141] Aristegui Noticias. *"La casa blanca de Enrique Peña Nieto*". [En línea]. https://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/. [Página consultada el 15/I/2020].

[142] Aristegui Noticias. *La historia que cambió el sexenio.* [En línea]. https://aristeguinoticias.com/2403/mexico/la-historia-de-la-casa-que-cambio-la-historia-del-sexenio/. [Página consultada el 14/I/2020].

Figura 19. Relación de mensajes dirigidos a Aristegui Noticias

6.2 RELACIÓN DE MENSAJES DIRIGIDOS A ARISTEGUI NOTICIAS

MENSAJES DIRIGIDOS A ARISTEGUI NOTICIAS
(enero de 2015 - julio de 2016)

FECHA	OBJETIVOS	MENSAJE	DOMINIO NSO *
12/1/2015	*Carmen Aristegui*	El siguiente mensaje no ha sido enviado [enlace malicioso]	*hxxp://smscentro[.]com (vía bit.ly)*
12/4/2015	*Carmen Aristegui*	Notificación de compra con tarjeta **** monto $3,500.00 M.N, ver detalles en: [enlace malicioso]	*hxxp://smsmensaje[.]mx*
8/5/2015	*Carmen Aristegui*	Aviso de vencimiento de pago asociado a tu servicio con cargo a tu tarjeta ****, ver mas detalles: [enlace malicioso]	*hxxp://smsmensaje[.]mx*
8/5/2015	*Carmen Aristegui*	Haz realizado un Retiro/Compra en Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: [enlace malicioso]	*hxxp://smsmensaje[.]mx*
11/5/2015	*Carmen Aristegui*	Estimado cliente informamos que presentas un problema de pago asociado a tu servicio, ver detalles.. [enlace malicioso]	*hxxp://smsmensaje[.]mx*
13/5/2015	*Carmen Aristegui*	UNONOTICIAS. [contenido omitido] [enlace malicioso]	*hxxp://unonoticias[.]net*
26/7/2015	*Carmen Aristegui*	UNOTV.COM/ ANONYMUS ANUNCIA QUE ATACARA PAGINA DE ARISTEGUI VER DETALLES: [enlace malicioso]	*hxxp://smsmensaje[.]mx*
26/7/2015	*Carmen Aristegui*	Haz realizado un Retiro/Compra en Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: [enlace malicioso]	*hxxp://unonoticias[.]net*
20/8/2015	*Carmen Aristegui*	IUSACELL/ Estimado cliente su factura esta lista, agradeceremos pago puntual por $17401.25	*hxxp://iusacell-movil[.]com.mx*
20/8/2015	*Carmen Aristegui*	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
22/8/2015	*Carmen Aristegui*	IUSACELL.COM/ EL SIGUIENTE MENSAJE ESTA MARCADO COMO URGENTE REVISALO DESDE NUESTRO PORTAL VER [enlace malicioso]	*hxxp://iusacell-movil[.]com.mx*

24/8/2015	*Carmen Aristegui*	ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA [contenido omitido]. DETALLES [enlace malicioso]	*hxxp://mymensaje-sms[.]com (vía bit.ly)*
30/8/2015	*Emilio Aristegui*	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [enlace malicioso)	*hxxp://unonoticias[.]net (vía bit.ly)*
30/8/2015	*Emilio Aristegui*	UNOTV.COM/ PRESIDENCIA DEMANDARÁ POR DIFAMACIÓN A QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. NOTA: [enlace malicioso]	*hxxp://unonoticias[.]net*
30/8/2015	*Emilio Aristegui*	UNOTV.COM/ DETIENEN A PRESUNTO LIDER DE CARTEL DE SINALOA EN [contenido omitido] VER: [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
30/8/2015	*Rafael Cabrera*	UNOTV.COM/ PRESIDENCIA DEMANDARA POR DIFAMACION A QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. NOTA: [enlace malicioso]	*hxxp://fb-accounts[.]com (vía bit.ly)*
30/8/2015	*Rafael Cabrera*	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [enlace malicioso]	*hxxp://unonoticias[.]net (vía bit.ly)*
25/10/2015	*Carmen Aristegui*	Hola te envio invitacion electronica con detalles por motivo de mi fiesta de disfraces espero contar contigo alonso: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía tinyurl.com)*

FECHA	OBJETIVOS	MENSAJE	DOMINIO NSO *
9/2/2016	*Carmen Aristegui*	Carmen hace 5 dias que no aparece mi hija te agradecere mucho que compartas su foto, estamos desesperados: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
10/2/2016	*Carmen Aristegui*	Querida Carmen fallecio mi hermano en un accidente, estoy devastada, envio datos del velorio, espero asistas: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
24/2/2016	*Carmen Aristegui*	UNOTV.COM/ LANZA TELEVISA DESPLEGADOS EN TODOS SUS MEDIOS;CRITICA POSTURA DE ORGANIZACION ARTICULO 19. VER: [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
18/3/2016	*Emilio Aristegui*	UNOTV.COM/ EN ENTREVISTA PARA DIARIO DE EU; MIGUEL ANGEL MANCERA ACEPTA SU HOMOSEXUALIDAD. DETALLES: [enlace malicioso]	*hxxp://unonoticias[.]net*
1/4/2016	*Emilio Aristegui*	ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS, SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MÁS IMPORTANTES: [enlace malicioso]	*hxxp://unonoticias[.]net*
6/4/2016	*Emilio Aristegui*	ARISTEGUINOTICIASONLINE.MX ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: [enlace malicioso]	*hxxps://smsmensaje[.]mx*
11/5/2016	*Emilio Aristegui*	UNOTV.COM/ CONFIRMA PGR QUE HIJO MAYOR DE AMLO LLEVA 48 HRS DESAPARECIDO. DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
12/5/2016	*Sebastián Barragán*	Tengo pruebas clave y fidedignas en contra de servidores publicos, ayudame tiene que ver con este asunto [enlace malicioso]	*hxxps://secure-access10[.]mx (vía bit.ly)*
16/5/2016	*Emilio Aristegui*	UNOTV.COM/ ASESINAN AL CITY MANAGER ARNE DEN RUHEN. DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net*
18/5/2016	*Rafael Cabrera*	TELCEL.COM/ EL SIGUIENTE MENSAJE SE HA MARCADO COMO URGENTE Y NO SE RECIBIO COMPLETAMENTE RECUPERELO EN [enlace malicioso]	*hxxps://smsmensaje[.]mx (vía bit.ly)*
18/5/2016	*Emilio Aristegui*	UNOTV.COM/ FILTRAN VIDEO DONDE LORET DE MOLA MANTIENE RELACIONES SEXUALES CON PAOLA ROJAS. VER VIDEO [enlace malicioso]	*hxxps://unonoticias[.]net*
19/5/2016	*Rafael Cabrera*	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE $8,854.90 M/N VERIFIQUE DETALLES: [enlace malicioso]	*hxxps://ideas-telcel.com[.]mx*
19/5/2016	*Emilio Aristegui*	UNOTV.COM/ POSIBLE CORRUPCION REVELA AUDIO TELEFONICO ENTRE EPN Y PRESIDENTE DE OHL. AUDIO EN: [enlace malicioso]	*hxxps://unonoticias[.]net*
20/5/2016	*Rafael Cabrera*	Facebook reporta intentos de acceso a la cuenta: Rafa Cabrera. Evite bloqueo de cuenta, verifique en: [enlace malicioso]	*hxxps://fb-accounts[.]com*

FECHA	OBJETIVOS	MENSAJE	DOMINIO NSO *
20/5/2016	*Emilio Aristegui*	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE $10,854.90 M/N VERIFIQUE DETALLES [enlace malicioso]	*hxxps://ideas-telcel[.]com.mx*
23/5/2016	*Rafael Cabrera*	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net*
23/5/2016	*Emilio Aristegui*	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net*
24/5/2016	*Rafael Cabrera*	No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como cojemos bn rico y en tu cama: [enlace malicioso]	*hxxps://smsmensaje[.]mx (vía bit.ly)*
26/5/2016	*Emilio Aristegui*	UNOTV.COM/ HAYAN DECAPITADO A PERIODISTA EN VERACRUZ Y DEJAN NARCOMENSAJE AMENAZADOR. FOTOS Y DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net*
27/5/2016	*Emilio Aristegui*	UNOTV.COM/ DECOMISAN CARGAMENTO DEL CIDA/ OSAMA BIN LADEN NO HA MUERTO/ DETIENEN A LUPITA DALESIO [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
30/5/2016	*Emilio Aristegui*	UNOTV.COM/ EJECUTAN PERIODISTA Y DEJAN NARCOMENSAJE/ CONTINUA DOBLE NO CIRCULA/ NOVIA ENLOQUECE DE CELOS [enlace malicioso]	*hxxps://smsmensaje[.]mx (vía bit.ly)*
1/6/2016	*Emilio Aristegui*	UNOTV.COM/ CARMEN ARISTEGUI SE DESTAPA COMO CANDIDATA AL GOBIERNO DE LA CDMX PARA EL 2018. DETALLES: [enlace malicioso]	*hxxps://unonoticias[.]net*
3/6/2016	*Carmen Aristegui*	Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: [enlace malicioso]	*hxxp://smsmensaje[.]mx*
3/6/2016	*Emilio Aristegui*	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA VER DETALLES: [enlace malicioso]	*hxxps://smsmensaje[.]mx (vía bit.ly)*
13/6/2016	*Carmen Aristegui*	Hace 3 días que no aparece mi hija, estamos desesperados, te agradecere que me ayudes a compartir su foto: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
15/6/2016	*Carmen Aristegui*	Buenas tardes Carmen, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
22/6/2016	*Emilio Aristegui*	UNOTV.COM/ REVELAN VIDEO DONDE CRISTIANO RONALDO SE ENFADA Y AVIENTA MICROFONO DE REPORTERO. VIDEO EN [enlace malicioso]	*hxxps://unonoticias[.]net*

FECHA	OBJETIVOS	MENSAJE	DOMINIO NSO *
28/6/2016	*Carmen Aristegui*	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/ FALLECE CHACHITA [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
28/6/2016	*Emilio Aristegui*	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/ FALLECE CHACHITA [enlace malicioso]	*hxxps://smsmensaje[.]mx (vía bit.ly)*
4/7/2016	*Carmen Aristegui*	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
4/7/2016	*Emilio Aristegui*	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [enlace malicioso]	*hxxps://unonoticias[.]net (vía bit.ly)*
12/7/2016	*Emilio Aristegui*	UNOTV.COM/ FILMAN A REPORTERO Y PERIODISTA CUANDO SON LEVANTADOS POR COMANDO ARMADO EN TAMAULIPAS. VIDEO: [enlace malicioso]	*hxxps://unonoticias[.]net*
15/7/2016	*Carmen Aristegui*	[Contenido omitido] [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
18/7/2016	*Emilio Aristegui*	Hola oye abriste nuevo facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: [enlace malicioso]	*hxxp://fb-accounts[.]com*
19/7/2016	*Carmen Aristegui*	Hola buen martes. Oye que pedo con el puto Lopez Doriga? Mira lo que escribió sobre ti hoy, urge desmentirlo: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
23/7/2016	*Emilio Aristegui*	Amigo, hay una pseudo cuenta de fb y twitter identica a la tuya checala para que la denuncies mira checala: [enlace malicioso]	*hxxp://fb-accounts[.]com*
25/7/2016	*Carmen Aristegui*	Bienvenido Club [contenido omitido], se ha aplicado un cargo de $875.85 a su linea, si desea cancelar ingrese a: [enlace malicioso]	*hxxp://smsmensaje[.]mx (vía bit.ly)*
28/7/2016	*Emilio Aristegui*	UNOTV.COM/ VIRAL EL VIDEO DE FUERTE GOLPE QUE RECIBE EN LA CARA OSORIO CHONG PROPINADO POR MAESTRO. VIDEO: [enlace malicioso]	*hxxps://unonoticias[.]net*

* En varios casos, el atacante utilizó un servicio de acortamiento de direcciones URL para ocultar el dominio relacionado a la infraestructura de Pegasus. Se indica entre paréntesis cuál usó.

Fuente: Article19, R3D y SOCIAL TIC. Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. [En línea]. https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf. [Página consultada el 14/I/2020].

Como se sabe, el gobierno de México negó, por conducto del entonces vocero de la Presidencia, Eduardo Sánchez a través de su cuenta de Twitter, los señalamientos a periodistas, con un comunicado en el que rechazó que existan pruebas que relacionen al gobierno mexicano con el uso del *software* de espionaje. En dicho texto se podía leer:

> Para el Gobierno de la República, el respeto a la privacidad y la protección de datos personales de todos los individuos son valores inherentes a nuestra libertad, democracia y Estado de Derecho. Por tanto, condenamos cualquier intento de vulnerar el derecho a la privacidad de cualquier persona[143].

La crítica a la publicación por parte del vocero de la Presidencia es que, en el texto, no se negó la compra del software por el gobierno federal, y tampoco se descarta la posibilidad de que se haya hecho el espionaje.

Cabe señalar que, otros sonados casos en la sociedad mexicana sobre espionaje son los padecidos por otros periodistas, uno de ellos Carlos Loret de Mola, incluso podríamos tener una lista interminable de amenazas digitales que atentan contra los derechos humanos, sin embargo, este tipo de amenazada se lleva a cabo mediante un *software* altamente peligroso para la sociedad.

Sin duda alguna, se puede decir que, por las características de alta invasión, las facultades de vigilancia gubernamental deben estar estricta y detalladamente reguladas en una ley formal y material. En este sentido, no puede considerarse que las normas que contemplan la intervención de comunicaciones privadas constituyan base legal suficiente para la utilización de herramientas tan poderosas e invasivas como los ataques con *malware* de espionaje. Por lo tanto, la utilización de estas herramientas, sin una norma legal que las regule específicamente debe considerarse violatoria de los derechos humanos.

Culminemos la exposición de este famoso caso de espionaje en México, señalando que, es lógico que da demasiado por escribir y analizar, sin embargo, para finalizar, tomemos las palabras que la misma periodista Carmen Aristegui expresó en una conferencia de prensa efectuada en junio de 2017 donde increpó al entonces presidente Enrique Peña Nieto, mencionando: "¿Para qué quería la información de un adolescente?", ¿de qué más es capaz, presidente siniestro?".[144]

---

[143] AZ Noticias. Presidencia de México niega espionaje del que se le acusa. [En línea]. https://aznoticias.mx/index.php/mexico-movil/23868-presidencia-de-mexico-niega-el-espionaje-del-que-se-le-acusa [Página consultada el 26/VII/ 2019]

[144] Proceso. "¿De qué más es capaz, presidente siniestro?: Aristegui". En línea]. https://www.proceso.com.mx/491688/capaz-presidente-siniestro-aristegui [Página consultada el 27/VII/ 2019].

Como una primera reflexión sobre los casos de espionaje comentados en este capítulo, se puede decir que, no existe la menor duda de que dicha actividad es llevada a cabo en nuestro país, lógicamente, al margen de cualquier instrumento que lo pudiera prohibir. Efectivamente es una acción que viola los derechos humanos, como lo dijo en su momento el Ombudsman nacional, Luis Raúl González Pérez.

También, hay que tomar en cuenta que, el futuro del espionaje en nuestro país es incierto y mucho debate ha provocado, por ejemplo, se ha dicho que en lugar del CISEN:

> Lo ideal sería replantear la creación de una Agencia Mexicana de Inteligencia con mayores niveles de independencia política de la Secretaría de Gobernación, su titular podría ser ratificado por dos terceras partes del Senado y sus facultades deberían estar exclusivamente delimitadas a las establecidas por la ley[145].

"Destacados defensores de derechos humanos, periodistas y activistas anticorrupción de México han sido afectados por un avanzado programa de espionaje adquirido por el gobierno mexicano que, en teoría, solo debe ser utilizado para investigar a criminales y terroristas"[146].

Es un entorno complejo el punto en el que nos encontramos ya que actualmente la sociedad y los derechos humanos, así como las garantías individuales parecen ser los nuevos enemigos del gobierno, refiriéndonos al ámbito nacional. A pesar de las múltiples investigaciones que se llevan y llevaron a cabo en torno a los temas, el gobierno de Peña Nieto no pudo desmentir ni justificar la versión de los hechos en la que son señalados socialmente como agresión a la privacidad y al uso de herramientas digitales para amedrentar a ciudadanos mexicanos.

---

[145] El Heraldo de México. Espionaje y futuro del CISEN. [En línea]. https://heraldodemexico.com.mx/opinion/espionaje-y-futuro-del-cisen/ [Página consultada el 26/VII/ 2019].

[146] The New York Times. *"Somos los nuevos enemigos del Estado: el espionaje a activistas y periodistas en México"*. [En línea]. https://www.nytimes.com/es/2017/06/19/espanol/america-latina/mexico-*Pegasus*-nso-group-espionaje.html. [Página consultada el 26/VII/ 2019].

4. CASO PRÁCTICO SOBRE CONOCIMIENTO DE ESPIONAJE A NIVEL PERSONAL E INTERNACIONAL.

En este capítulo, se ha recaudado información mediante encuestas de personas que de alguna manera podría estar al tanto de los métodos, artículos, aplicaciones y temas en torno a la vigilancia actual. Se ha seleccionado un universo de 50 personas de las cuales 25 son estudiantes de la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México y 25 son personas con estudios y que cuentan con un empleo fijo.

Las preguntas del caso giran en torno a reflejar su opinión en cuánto a los acontecimientos de los casos de vigilancia a través de software y de como lo reflejan en su día a día, desde el uso de su celular hasta la opinión sobre una reglamentación. Si bien, el universo es variado, podremos sacar conclusiones en cuanto a que tipo de afección tiene la atención de las personas sobre este tema o si definitivamente no tiene importancia alguna en sus vidas.

4.1. Selección del universo, población y muestra

"Hernández, Fernández y Baptista (2006) explican que, para seleccionar una muestra, primero se deberá definir la unidad de análisis, ya sea personas, organizaciones, comunidades, situaciones, etc., por lo que sobre qué o quiénes se recolectarán datos dependerá del planteamiento del problema a investigar y de los alcances del estudio. Una vez realizado esto, se delimita la población. Misma que se entiende como "el conjunto de todos los casos que concuerdan con una serie de especificaciones".[147]

Considérese que, un estudio no será mejor por tener un número de resultados más grande, sino que la calidad de un trabajo de investigación consiste en delimitar la población con base en el planteamiento del problema.

Es necesario destacar que, las muestras pueden ser de dos tipos: probabilísticas y no probabilísticas. "La muestra probabilística es un subgrupo de la población en el que todos los elementos de ésta tienen la misma posibilidad de ser elegidos. En este tipo de

[147] R Hernández Sampieri, Fernández-Collado, C. Baptista, Lucio, P. *Metodología de la investigación*. Ed. Mc Graw Hill, México, p. 238.

muestras, se requieren dos elementos: determinar el tamaño de la muestra y seleccionar los elementos muestrales en forma aleatoria."[148].

Por su parte, la muestra no probabilística o dirigida es un subgrupo de la población en el que la elección de los elementos no depende de la probabilidad, sino de las características de la investigación[149].

En este último tipo de muestras, interviene el criterio y/o decisión de las personas. Por tanto, una vez aclarados estos conceptos, en el presente trabajo se tiene:

Unidad de análisis	Personas
Cantidad	50
Universo	Habitantes de la CDMX.
Población	Empleados en general y estudiantes de licenciatura de la FCPyS
Tipo de muestra	Probabilística

4.2. Presentación de la herramienta de diagnóstico

Se realizó un cuestionario con 13 reactivos y se integraron preguntas realizadas en un análisis de Animal Político en torno a la población mexicana que opina sobre si el gobierno los espía, mismo que se presenta en el Anexo A. El diseño del cuestionario del presente trabajo fue producto del análisis de los tópicos estudiados y es una aportación de la sustentante con base en el interés que se tiene respecto a las hipótesis, objetivos y preguntas planteadas.

4.3. Descripción del proceso de recolección de datos

La recolección de datos se llevó a cabo del 07 de septiembre al 17 de octubre de 2019. Cabe resaltar que previa participación individual de quienes dieron respuesta a la herramienta, se platicó con los mismos explicándoles el objetivo del cuestionario, por lo que dichas personas estuvieron de acuerdo, otorgando el permiso para proceder al estudio.

[148]E-uaem. *Selección de la muestra*. [En línea]. http://euaem1.uaem.mx/bitstream/handle/123456789/2776/506_6.pdf?sequence=1&isAllowed=y. [Página consultada el 26/I/ 2020].
[149]*Ibidem.*

4.4. Tablas de captura y análisis

En primer término, se presentan las tablas de Excel que se diseñaron para la captura de las respuestas. Posteriormente se expone cada uno de los cuestionamientos con su respectiva gráfica e interpretación.

Análisis de cuestionario de caso de estudio realizado a profesionistas con trabajo en empresas privadas, de gobierno o independientes.

Como se observa, la edad promedio de los empleados es de 30 años con seis meses, de los cuales 13 fueron del sexo femenino y 12 masculino. Además, tres cuentan con Maestría, 21 con Licenciatura y uno con Preparatoria. Dos son empleados de gobierno, veinte de la iniciativa privada y tres son profesionistas independientes.

Tabla 8. Cuadro de elaboración propia con información proporcionada por los encuestados.

Datos del participante - EMPLEADOS															
Nombre	Edad	Sexo		Nivel de estudios						Actividad					
		Femenino	Masculino	Doctorado	Maestría	Licenciatura	Prepa	Secundaria	Primaria	Empleado de gobierno	Empleado iniciativa privada	Profesionista independiente	Estudiante	Empresario	Otro
Marcela G. L.	29	1				1						1			
Mariana Itzael C. V.	28	1				1				1					
Aldo L. R.	29		1			1						1			
Daniel Alberto D. L.	25		1			1					1				
María de la Luz S. C.	33	1			1					1					
Miguel C.	36		1			1					1				
Víctor R.	28		1			1					1				
Luis E.	30		1			1					1				
Atziry Pamela D. B.	28	1				1					1				
Claudia C. c.	27	1			1						1				
Iker B. S.	25		1			1					1				
Iván C.	39		1			1						1			
Rodolfo B. A.	25		1			1					1				
Nadia R. N.	31	1				1					1				
Amellaly B. T.	25	1				1					1				
Antonieta J.	40	1					1				1				
Cinthia M. L.	31	1				1					1				
Erick Omar C. L.	30		1			1					1				
Laura R. M.	36	1			1						1				
Christian G.	34		1			1					1				
Ana Victoria Z.	25	1				1					1				
Karla S.	31	1				1					1				
Alicia O.	38	1				1					1				
Osiris I. O.	31		1			1					1				
Héctor Antonio P. I.	30		1			1					1				
	30.6	**13**	**12**	**0**	**3**	**21**	**1**	**0**	**0**	**2**	**20**	**3**	**0**	**0**	**0**

Tabla 9. Preguntas 1-4 de Caso práctico. Preguntas tomadas de: Animal Político.

Datos del participante - EMPLEADOS	Pregunta 1.		Pregunta 2.			Pregunta 3.			Pregunta 4.		
Nombre	¿Usted se enteró del caso del exempleado de la agencia de seguridad de Estados Unidos Edward Snowden, que denunció una red de espionaje de llamadas telefónicas, correos electrónicos y mensajes en redes sociales que hace ese país al resto del mundo?		¿Usted cree que en México existe espionaje por parte del gobierno hacia los ciudadanos?			En su opinión, ¿para garantizar la seguridad de un país, se justifica o no se justifica que el gobierno de un país espíe a otros países?			En su opinión, ¿para garantizar la seguridad de sus ciudadanos, se justifica o no se justifica que el gobierno espíe a sus propios ciudadanos?		
	No se enteró	Sí se enteró	No existe	Sí existe	No sé	Sí se justifica	No se justifica	No sabe	Sí se justifica	No se justifica	No sabe
Marcela G. L.	1			1				1		1	
Mariana Itzael C. V.		1		1		1				1	
Aldo L. R.		1		1		1			1		
Daniel Alberto D. L.		1		1			1			1	
María de la Luz S. C.		1		1			1			1	
Miguel C.	1				1		1			1	
Víctor R.		1		1			1			1	
Luis E.		1		1		1			1		
Atziry Pamela D. B.		1		1		1			1		
Claudia C. c.	1			1		1				1	
Iker B. S.		1			1	1				1	
Iván C.		1		1			1			1	
Rodolfo B. A.		1		1			1			1	
Nadia R. N.	1			1			1			1	
Amellaly B. T.	1			1			1			1	
Antonieta J.		1		1			1			1	
Cinthia M. L.	1			1			1			1	
Erick Omar C. L.		1	1				1			1	
Laura R. M.		1		1			1			1	
Christian G.		1		1		1			1		
Ana Victoria Z.		1		1			1			1	
Karla S.		1		1			1			1	
Alicia O.		1		1			1			1	
Osiris I. O.		1		1			1			1	
Héctor Antonio P. I.		1		1		1			1		
	6 **24%**	**19** **76%**	**1** **4%**	**22** **88%**	**2** **8%**	**8** **31%**	**16** **64%**	**1** **4%**	**5** **20%**	**20** **80%**	**0**

Fuente: Animal Político. 59% de los mexicanos cree que el gobierno los espía: Parametría. [En línea]. https://www.animalpolitico.com/2013/07/59-de-los-mexicanos-cree-que-el-gobierno-los-espia-parametria/. [Página consultada el 26/IX/ 2019].

Con relación al caso Snowden, el 76% sí se enteró. El 88% reconoce que el gobierno espía a los ciudadanos y el 64% no justifica tal acción respecto de un país a otro, mientras que el 32% sí lo justifica. Con relación a que el gobierno efectúe espionaje a sus ciudadanos, el 80% no lo justifica y el 20% restante sí.

Tabla 10. Preguntas 5-8 de elaboración propia.

Datos del participante - EMPLEADOS	Pregunta 5.			Pregunta 6.						Pregunta 7.				Pregunta 8.		
Nombre	En octubre de 2013, la revista alemana Der Spiegel reveló, con base en documentos facilitados por Edward Snowden, que desde 2010 funcionarios mexicanos (Felipe Calderón e integrantes de la extinta Secretaría de Seguridad Pública) habían sido vigilados por el gobierno de Estados Unidos. ¿Usted considera que Estados Unidos continuará espiando a los presidentes mexicanos?			¿Cuál cree que sea la razón principal por la que Estados Unidos espía a los líderes mundiales?						¿Qué tan común cree que sea en México que los políticos espíen y graben las conversaciones de otros políticos?				¿Usted está de acuerdo o desacuerdo que los políticos espíen y graben las conversaciones de otros políticos?		
	Lo seguirá haciendo	No lo seguirá haciendo	No sé	Mantener el control mundial	Informarse de las estrategias y planes de otros países	Evitar ataques terroristas	Mantener sus intereses económicos	Ver qué tan corruptos son	f)No sé	Muy común	Algo común	Poco común	Nada común	De acuerdo	En desacuerdo	No me interesa
Marcela G. L.	1						1					1			1	
Mariana Itzael C. V.	1						1			1				1		
Aldo L. R.			1	1						1				1		
Daniel Alberto D. L.	1						1			1				1		
María de la Luz S. C.	1				1					1					1	
Miguel C.	1						1				1				1	
Víctor R.	1					1					1				1	
Luis E.	1						1			1				1		
Atziry Pamela D. B.	1			1						1				1		
Claudia C. c.	1			1						1						1
Iker B. S.			1	1							1					1
Iván C.	1			1						1				1		
Rodolfo B. A.	1			1							1					1
Nadia R. N.	1			1						1				1		
Amellaly B. T.	1			1						1					1	
Antonieta J.	1			1							1				1	
Cinthia M. L.			1		1						1			1		
Erick Omar C. L.	1						1				1				1	
Laura R. M.	1						1			1					1	
Christian G.	1						1				1				1	
Ana Victoria Z.	1			1							1					1
Karla S.	1			1						1					1	
Alicia O.	1			1						1						1
Osiris I. O.	1			1						1					1	
Héctor Antonio P. I.	1						1			1					1	
	22	**0**	**3**	**13**	**2**	**1**	**9**	**0**	**0**	**15**	**9**	**1**	**0**	**8**	**12**	**5**
	88%		**12%**	**52%**	**8%**	**4%**	**36%**			**60%**	**36%**	**4%**		**32%**	**48%**	**20%**

El 88% de esta muestra expresa que los Estados Unidos seguirán expiando a los presidentes mexicanos y solamente tres casos no saben. El mayor porcentaje (52%)

señalan que tal situación lleva a Estados Unidos a mantener el control mundial. Por su parte, el 60% reconoce que el espionaje es común en la política, estando el 32% a favor y el 48% en contra.

Tabla 11. Preguntas 9-13 de elaboración propia.

Datos del participante - EMPLEADOS	Pregunta 9.			Pregunta 10.			Pregunta 11.			Pregunta 12.			Pregunta 13.		
Nombre	¿Usted está de acuerdo o desacuerdo que el espionaje generalizado mediante el uso de la tecnología es una violación a los Derechos Humanos?			¿Usted está de acuerdo o desacuerdo que a nivel internacional, no exista reglamentación suficiente que proteja los DH de los ciudadanos en contra del uso de la tecnología de espionaje?			¿Usted está de acuerdo o desacuerdo que la invasión de privacidad, el uso de datos personales sin autorización, la intervención ilegal en las comunicaciones, el espionaje de personas y el uso de información para lograr objetivos en contra de individuos, son prácticas violatorias de los Derechos Humanos?			¿Usted está de acuerdo o desacuerdo que la vigilancia por medios tecnológicos es una vía para que los gobiernos logren mantener sociedades controladas?			¿Qué tanto considera está haciendo la comunidad internacional para proteger a los ciudadanos del mal uso de la tecnología de espionaje?		
	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	Mucho	Muy poco	Nada
Marcela G. L.	1				1		1			1					1
Mariana Itzael C. V.	1			1			1			1				1	
Aldo L. R.	1			1				1			1				1
Daniel Alberto D. L.	1			1			1				1				1
María de la Luz S. C.	1			1			1				1				1
Miguel C.	1				1		1			1				1	
Víctor R.	1				1		1				1			1	
Luis E.		1		1			1				1			1	
Atziry Pamela D. B.		1		1			1				1			1	
Claudia C. c.	1				1		1				1			1	
Iker B. S.	1				1		1			1				1	
Iván C.	1			1			1			1				1	
Rodolfo B. A.	1				1		1			1				1	
Nadia R. N.	1				1		1			1				1	
Amellaly B. T.	1				1		1			1				1	
Antonieta J.	1				1		1			1				1	
Cinthia M. L.	1			1			1			1					1
Erick Omar C. L.	1			1			1			1				1	
Laura R. M.	1				1		1				1			1	
Christian G.		1		1			1			1				1	
Ana Victoria Z.	1			1			1			1				1	
Karla S.		1			1		1			1					1
Alicia O.	1			1			1				1			1	
Osiris I. O.	1					1	1			1					1
Héctor Antonio P. I.	1			1			1			1				1	
	21	**4**	**0**	**13**	**11**	**1**	**24**	**1**	**0**	**16**	**9**	**0**	**0**	**18**	**7**
	84%	**16%**	**0%**	**52%**	**44%**	**4%**	**96%**	**4%**	**0%**	**64%**	**36%**	**0%**	**0%**	**72%**	**28%**

El 84% reconoce que el espionaje es una violación a los Derechos Humanos, y llama la atención que un 52% está de acuerdo en que no existe reglamentación a nivel internacional en dicho aspecto, mientras que el 48% manifiesta desacuerdo. El 64% manifiesta estar de

acuerdo en que la vigilancia facilita el control de las sociedades y el 72% señala que la comunidad internacional está haciendo muy poco para proteger a la ciudadanía de dicho fenómeno.

Tabla 12. Cuadro de elaboración propia con información obtenida en las encuestas realizadas.

¿Qué propuestas le parecen viables para regular en nuestro país las actividades de espionaje tecnológico?
- Primero habría que regular el sector de tecnologías. - Implementar campañas de difusión de información sobre la protección de datos personales. - Que investiguen únicamente a la gente del gobierno y posibles delincuentes. - Hacer más regulaciones en materia de vigilancia internacional. - Leyes que especifiquen los términos permitidos. - Legislación para castigar dichas actividades. - Condenas fuertes a personas que usen el espionaje para fines fuera de política o seguridad. - Crear una regulación la cual establezca las condiciones, así como el uso de dicha información obtenida. - Crear una ley en donde especifique hasta qué punto aplica y puede llegar el espionaje. - Tener una mejor infraestructura para el control de datos personales. - Regulaciones en las empresas privadas de telecomunicaciones. - Ligar, en caso de celulares, el código IMEI a cada usuario para identificar la procedencia de la información. - Que no existan cookies o que se controlen. - Crear un organismo que se dedique a vigilar esas prácticas. - Penalizar el mal uso de datos o información de usuarios para fines de lucro, políticos o espionaje. - **Hacer una regulación internacional en la que se tengan lineamientos, reglas y todo tipo de regulaciones.** - Es algo que no debería ser regulado porque no debería existir el espionaje. - Crear marco normativo para el manejo del *Big Data* tanto para sector público como privado.

Como se observa, las respuestas son diversas, sin embargo, prevalece la idea de la necesidad de crear regulaciones al respecto. Llama la atención la respuesta marcada con **negritas**, pues bajo tal parámetro *los delitos no deberían regularse porque no deberían existir* (aseveración propia).

Análisis de caso de estudio realizado a estudiantes de Licenciatura en la UNAM.

Tabla 13. Cuadro de elaboración propia con información proporcionada por los encuestados.

Datos del participante - ESTUDIANTES									
Nombre	Edad	Sexo		Nivel de estudios					
		Femenino	Masculino	Doctorado	Maestría	Licenciatura	Prepa	Secundaria	Primaria
Samantha J. A.	19	1				1			
María Fernanda L. A.	21	1				1			
Laura O.	20	1				1			
Eliot M. M.	22		1			1			
Yesenia V.	23	1				1			
Cristian B.	20		1			1			
Diana S. C.	18	1				1			
Rafael S. B.	18		1			1			
Yazmín L. V.	18	1				1			
Ximena P.	19	1				1			
María Fernanda r. T.	18	1				1			
Rodolfo R. L.	21		1			1			
Erika Pepita B. U.	21	1				1			
Samantha P.	18	1				1			
Elena R. M.	20	1				1			
Dayana F. L.	19	1				1			
Cinthya G.	20	1				1			
Nora Elia A. R	20	1				1			
Muhamed C.	19		1			1			
Javier N.	21		1			1			
Víctor P.	27		1			1			
Julieta F. M.	21	1				1			
Jimena R. O.	22	1				1			
Victoria R.	20	1				1			
Ricardo D,	20		1			1			
	20.2	**17**	**8**	**0**	**0**	**25**	**0**	**0**	**0**

En este caso, los estudiantes tienen una edad promedio de veinte años, siendo diecisiete mujeres y ocho varones. Todos están estudiando la Licenciatura en UNAM Ciudad Universitaria.

Tabla 14. Preguntas 1-4 de Caso práctico. Preguntas tomadas de: Animal Político

Datos del participante - ESTUDIANTES										Pregunta 1.		Pregunta 2.			Pregunta 3.			Pregunta 4.		
Nombre	Edad	Sexo		Nivel de estudios						¿Usted se enteró del caso del exempleado de la agencia de seguridad de Estados Unidos Edward Snowden, que denunció una red de espionaje de llamadas telefónicas, correos electrónicos y mensajes en redes sociales que hace ese país al resto del mundo?		¿Usted cree que en México existe espionaje por parte del gobierno hacia los ciudadanos?			En su opinión, ¿para garantizar la seguridad de un país, se justifica o no se justifica que el gobierno de un país espíe a otros países?			En su opinión, ¿para garantizar la seguridad de sus ciudadanos, se justifica o no se justifica que el gobierno espíe a sus propios ciudadanos?		
		Femenino	Masculino	Doctorado	Maestría	Licenciatura	Prepa	Secundaria	Primaria	No se enteró	Sí se enteró	No existe	Sí existe	No sé	Sí se justifica	No se justifica	No sabe	Sí se justifica	No se justifica	No sabe
Samantha J. A.	19	1				1				1			1		1				1	
María Fernanda L. A.	21	1				1				1			1		1				1	
Laura O.	20	1				1					1			1			1			1
Eliot M. M.	22		1			1					1		1		1			1		
Yesenia V.	23	1				1					1		1		1			1		
Cristian B.	20		1			1				1			1		1			1		
Diana S. C.	18	1				1					1		1			1			1	
Rafael S. B.	18		1			1				1			1			1			1	
Yazmín L. V.	18	1				1					1		1			1			1	
Ximena P.	19	1				1					1		1			1			1	
María Fernanda r. T.	18	1				1					1			1	1				1	
Rodolfo R. L.	21		1			1					1		1			1			1	
Erika Pepita B. U.	21	1				1				1			1			1			1	
Samantha P.	18	1				1					1		1		1				1	
Elena R. M.	20	1				1					1		1		1			1		
Dayana F. L.	19	1				1					1		1			1			1	
Cinthya G.	20	1				1				1			1			1			1	
Nora Elia A. R	20	1				1					1		1			1			1	
Muhamed C.	19		1			1					1		1			1		1		
Javier N.	21		1			1					1		1		1			1		
Víctor P.	27		1			1					1		1		1			1		
Julieta F. M.	21	1				1					1		1			1			1	
Jimena R. O.	22	1				1					1		1			1			1	
Victoria R.	20	1				1				1			1			1			1	
Ricardo D,	20		1			1				1				1		1			1	
	20.2	**17**	**8**	**0**	**0**	**25**	**0**	**0**	**0**	**8**	**17**	**0**	**22**	**3**	**10**	**14**	**1**	**7**	**17**	**1**
										32%	**68%**	**0%**	**88%**	**12%**	**40%**	**68%**	**4%**	**28%**	**68%**	**4%**

Fuente: Animal Político. 59% de los mexicanos cree que el gobierno los espía: Parametría. [En línea]. https://www.animalpolitico.com/2013/07/59-de-los-mexicanos-cree-que-el-gobierno-los-espia-parametria/. [Página consultada el 26/IX/ 2019].

El 68% sí se enteró del caso Snowden y el 32% no, porcentaje que se considera alto dado el carácter de estudiante. El 88% expresa que en nuestro país sí se efectúa espionaje por

parte del gobierno y en porcentajes cercanos, el 40% lo justifica y el 56% no cuando es de un país a otro. El 68% no justifica que en aras de la seguridad se practique el espionaje.

Tabla 15. Preguntas 5-8 de elaboración propia.

Datos del participante - ESTUDIANTES										Pregunta 5.			Pregunta 6.						Pregunta 7.				Pregunta 8.		
Nombre	Edad	Sexo		Nivel de estudios						En octubre de 2013, la revista alemana Der Spiegel reveló, con base en documentos facilitados por Edward Snowden, que desde 2010 funcionarios mexicanos (Felipe Calderón e integrantes de la extinta Secretaría de Seguridad Pública) habían sido vigilados por el gobierno de Estados Unidos. ¿Usted considera que Estados Unidos continuará espiando a los presidentes mexicanos?			¿Cuál cree que sea la razón principal por la que Estados Unidos espía a los líderes mundiales?						¿Qué tan común cree que sea en México que los políticos espíen y graben las conversaciones de otros políticos?				¿Usted está de acuerdo o desacuerdo que los políticos espíen y graben las conversaciones de otros políticos?		
		Femenino	Masculino	Doctorado	Maestría	Licenciatura	Prepa	Secundaria	Primaria	Lo seguirá haciendo	No lo seguirá haciendo	No sé	Mantener el control mundial	Informarse de las estrategias y planes de otros países	Evitar ataques terroristas	Mantener sus intereses económicos	Ver qué tan corruptos son	No sé	Muy común	Algo común	Poco común	Nada común	De acuerdo	En desacuerdo	No me interesa
Samantha J. A.	19	1				1				1			1							1				1	
María Fernanda L. A.	21	1				1				1			1							1				1	
Laura O.	20	1				1				1			1						1						1
Eliot M. M.	22		1			1				1			1							1			1		
Yesenia V.	23	1				1				1			1						1				1		
Cristian B.	20		1			1				1				1						1				1	
Diana S. C.	18	1				1						1		1						1				1	
Rafael S. B.	18		1			1						1	1						1					1	
Yazmín L. V.	18	1				1				1			1						1					1	
Ximena P.	19	1				1				1			1							1				1	
María Fernanda r. T.	18	1				1				1			1							1				1	
Rodolfo R. L.	21		1			1				1			1						1					1	
Erika Pepita B. U.	21	1				1						1				1				1				1	
Samantha P.	18	1				1				1						1				1					1
Elena R. M.	20	1				1				1						1				1					1
Dayana F. L.	19	1				1				1			1						1					1	
Cinthya G.	20	1				1				1			1						1					1	
Nora Elia A. R	20	1				1				1			1						1				1		
Muhamed C.	19		1			1				1			1							1			1		
Javier N.	21		1			1				1			1						1				1		
Víctor P.	27		1			1				1						1				1				1	
Julieta F. M.	21	1				1				1			1						1						1
Jimena R. O.	22	1				1				1						1				1					1
Victoria R.	20	1				1				1				1						1				1	
Ricardo D,	20		1			1				1						1				1					1
	20.2	**17**	**8**	**0**	**0**	**25**	**0**	**0**	**0**	**22**	**0**	**3**	**16**	**3**	**0**	**6**	**0**	**0**	**10**	**15**	**0**	**0**	**5**	**14**	**6**
										88%	**0%**	**12%**	**64%**	**12%**	**0%**	**24%**	**0**	**0**	**40%**	**60%**	**0%**	**0%**	**20%**	**56%**	**24%**

Solo tres casos consideran que los Estados Unidos no seguirá espiando a los Presidentes mexicanos contra 22 que expresan que se continuará haciendo. El 64% opina que ello es para que los Estados Unidos mantengan el control, el 24% para mantener intereses económicos y el 12% para conocer las estrategias de otros países. El 60% reconoce que en nuestro país es algo común que los políticos graben conversaciones de sus colegas y el 40% muy común. El 56% de la muestra está en desacuerdo con que el espionaje suceda y al 24% de la muestra no le interesa.

Tabla 16. Preguntas 9-13 de elaboración propia.

Datos del participante - ESTUDIANTES										Pregunta 9.			Pregunta 10.			Pregunta 11.			Pregunta 12.			Pregunta 13.		
Nombre	Edad	Sexo		Nivel de estudios						¿Usted está de acuerdo o desacuerdo que el espionaje generalizado mediante el uso de la tecnología es una violación a los Derechos Humanos?			¿Usted está de acuerdo o desacuerdo que a nivel internacional, no exista reglamentación suficiente que proteja los DH de los ciudadanos en contra del uso de la tecnología de espionaje?			¿Usted está de acuerdo o desacuerdo que la invasión de privacidad, el uso de datos personales sin autorización, la intervención ilegal en las comunicaciones, el espionaje de personas y el uso de información para lograr objetivos en contra de individuos, son prácticas violatorias de los Derechos Humanos?			¿Usted está de acuerdo o desacuerdo que la vigilancia por medios tecnológicos es una vía para que los gobiernos logren mantener sociedades controladas?			¿Qué tanto considera está haciendo la comunidad internacional para proteger a los ciudadanos del mal uso de la tecnología de espionaje?		
		Femenino	Masculino	Doctorado	Maestría	Licenciatura	Prepa	Secundaria	Primaria	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	De acuerdo	En desacuerdo	No sé	Mucho	Muy poco	Nada
Samantha J. A.	19	1				1				1				1		1			1				1	
María Fernanda L. A.	21	1				1				1				1		1			1					1
Laura O.	20	1				1						1		1		1			1				1	
Eliot M. M.	22		1			1				1			1			1			1				1	
Yesenia V.	23	1				1						1	1				1				1			1
Cristian B.	20		1			1					1			1		1				1			1	
Diana S. C.	18	1				1				1				1		1			1				1	
Rafael S. B.	18		1			1				1				1		1			1				1	
Yazmín L. V.	18	1				1				1				1		1			1					1
Ximena P.	19	1				1					1			1		1					1		1	
María Fernanda r. T.	18	1				1						1		1		1				1				1
Rodolfo R. L.	21		1			1				1				1		1			1				1	
Erika Pepita B. U.	21	1				1				1				1		1				1			1	
Samantha P.	18	1				1				1			1			1			1				1	
Elena R. M.	20	1				1				1			1			1			1					1
Dayana F. L.	19	1				1				1				1		1				1			1	
Cinthya G.	20	1				1				1				1		1			1					1
Nora Elia A. R	20	1				1				1				1		1			1				1	
Muhamed C.	19		1			1				1				1		1				1			1	
Javier N.	21		1			1				1				1		1			1			1		
Víctor P.	27		1			1				1				1		1			1				1	
Julieta F. M.	21	1				1				1			1			1			1					1
Jimena R. O.	22	1				1				1			1			1				1			1	
Victoria R.	20	1				1				1				1		1			1				1	
Ricardo D,	20		1			1				1			1			1				1			1	
	20.2	**17**	**8**	**0**	**0**	**25**	**0**	**0**	**0**	**20**	**2**	**3**	**7**	**18**	**0**	**24**	**1**	**0**	**16**	**7**	**2**	**1**	**17**	**7**
										80%	**8%**	**12%**	**28%**	**72%**	**0%**	**96%**	**4%**	**0%**	**64%**	**28%**	**8%**	**4%**	**68%**	**28%**

El 80% de los estudiantes expresa estar de acuerdo en que el espionaje viola los Derechos Humanos, llamando la atención que tres casos respondieron no sé. El 72% expresa estar en desacuerdo con regulación a la falta de reglamentación a nivel internacional y casi la totalidad (24 casos) que equivale al 96% señala que el espionaje es una violación a los Derechos Humanos. El 64% está de acuerdo en que el espionaje se hace con la finalidad de tener sociedades controladas y el 28% dice estar en desacuerdo. El 68% (17 casos) señalan que la comunidad internacional está haciendo muy poco con relación al tema de estudio.

Tabla 17. Cuadro de elaboración propia con información obtenida en las encuestas realizadas.

¿Qué propuestas le parecen viables para regular en nuestro país las actividades de espionaje tecnológico?
- Legislarlo. - Encriptación de información. - Crear una reglamentación. - La correcta aplicación de la ley de protección de datos personales. - **Restringir el acceso público y privado, haciendo que determinadas personas puedan relacionarse con unas cuantas.** - Hacer una difusión de los Derechos Humanos hacia la ciudadanía para que tengan muy claro cuáles son sus derechos. - Crear leyes que protejan a los ciudadanos del espionaje y que se castiguen los abusos. - Me parece viable que exista un documento que informe a los ciudadanos, asimismo nosotros podremos aceptar o estar enterados de la situación. - Reglamentar el uso de datos e información personal por parte de empresas. - **Justificar el por qué el gobierno toma este tipo de actividades.** - Penalizar el espionaje. - Mejorar las leyes de protección a datos personales. - **Creación de políticas públicas que brinden protección total de datos personales.** - **Una vez que se identifique el espionaje, crear una ley que lo sancione.** - **Tendría que analizarlo con más tiempo.** - Mayor control sobre la privacidad en redes sociales por parte del gobierno a los ciudadanos. - Regulación de decidir sobre tus datos. - Ley en contra de la violencia y difamación tecnológica. - Debería garantizarse seguridad en todos los aspectos. - Establecer un órgano más especializado en la materia. - Informar el uso de la Ley de Datos Personales.

En este caso, las respuestas parecen en ocasiones no tener sentido, como las marcadas en negritas. También se invita en diversas ocasiones a crear leyes y reglamentos al respecto.

Tabla 18. Cuadro comparativo entre resultados de empleados y estudiantes de Licenciatura de la UNAM. Preguntas 1-4 de Caso práctico: Preguntas tomadas de: Animal Político. Preguntas 5-13 de elaboración propia.

Comparativo (El dato que se incluye corresponde al mayor porcentaje de respuesta en cada caso).		
Pregunta	**Empleados**	**Estudiantes**

1. ¿Usted se enteró del caso del exempleado de la agencia de seguridad de Estados Unidos Edward Snowden, que denunció una red de espionaje de llamadas telefónicas, correos electrónicos y mensajes en redes sociales que hace ese país al resto del mundo?	**El 76%** Sí se enteró.	**El 68%** Sí se enteró.
Comentario: En ningún caso el porcentaje llega al 80% siendo menor el de los estudiantes, lo cual llama la atención, pues siendo temas de relevancia internacional sería deseable que la totalidad de los estudiantes estén inmersos en dichos eventos**.**		
2. ¿Usted cree que en México existe espionaje por parte del gobierno hacia los ciudadanos?	**El 88%** considera que sí existe.	**El 88%** considera que sí existe.
Comentario: En este caso el nivel de respuesta es el mismo, existiendo un gran convencimiento de que el espionaje es una acción común dentro del gobierno mexicano. Con estos porcentajes, es innegable que tal hecho sucede frecuentemente.		
3. En su opinión, ¿para garantizar la seguridad de un país, se justifica o no se justifica que el gobierno de un país espíe a otros países?	**El 64%** considera que no se justifica.	**El 56%** considera que no se justifica.
Comentario: Aunque la diferencia solamente es de un 12% entre la opinión de los empleados y los estudiantes, llama la atención que queda un abanico importante de personas que sí lo justifican.		
4. En su opinión, ¿para garantizar la seguridad de sus ciudadanos, se justifica o no se justifica que el gobierno espíe a sus propios ciudadanos?	**El 80%** considera que no se justifica.	**El 68%** considera que no se justifica.
Comentario: Aquí los porcentajes aumentan en ambas muestras, pero también, no existe u acuerdo generalizado al respecto.		
5. En octubre de 2013, la revista alemana Der Spiegel reveló, con base en documentos facilitados por Edward Snowden, que desde 2010 funcionarios mexicanos (Felipe Calderón e integrantes de la extinta Secretaría de Seguridad Pública) habían sido vigilados por el gobierno de Estados Unidos. ¿Usted considera que Estados Unidos continuará espiando a los presidentes mexicanos?	**El 88%** considera que lo seguirá haciendo.	**El 88%** considera que lo seguirá haciendo.
Comentario: Sin duda, la percepción de que los Estados Unidos continuará efectuando actividades de espionaje hacia los Presidentes de México es alta.		
6. ¿Cuál cree que sea la razón principal por la que Estados Unidos espía a los líderes mundiales?	**El 52%** considera que mantener el control mundial y **el 36%** mantener sus intereses económicos.	**El 64%** considera que mantener el control mundial y **el 24%** mantener sus intereses económicos.
Comentario: La idea de que los Estados Unidos desea mantener el control mundial es la más arraigada entre la población seguida de la percepción del interés económico.		

7. ¿Qué tan común cree que sea en México que los políticos espíen y graben las conversaciones de otros políticos?	**El 60%** lo considera muy común.	**El 60%** lo considera algo común.
Comentario: En ambas muestras se muestra un porcentaje igual con la idea de que es común que se haga espionaje a los políticos mexicanos		
8. ¿Usted está de acuerdo o desacuerdo que los políticos espíen y graben las conversaciones de otros políticos?	**El 48%** está en desacuerdo.	**El 56%** está en desacuerdo.
Comentario: Los porcentajes se quedan cerca del cincuenta por ciento en ambas poblaciones, lo que quiere decir que la otra mitad sí se identifica con la idea de tal actividad entre políticos.		
9. ¿Usted está de acuerdo o desacuerdo que el espionaje generalizado mediante el uso de la tecnología es una violación a los Derechos Humanos?	**El 84%** está de acuerdo.	**El 80%** está de acuerdo.
Comentario: La pregunta que surge en este caso, es ¿por qué el porcentaje restante no considera que el espionaje es una violación a los derechos Humanos?		
10. ¿Usted está de acuerdo o desacuerdo que a nivel internacional, no exista reglamentación suficiente que proteja los DH de los ciudadanos en contra del uso de la tecnología de espionaje?	**El 52%** está de acuerdo.	**El 72%** está en desacuerdo.
Comentario: En el caso de los empleados existe una dualidad, mientras que en el caso de los estudiantes 7 de dada 10 reconocen estar en desacuerdo con la falta de normatividad a nivel internacional.		
11. ¿Usted está de acuerdo o desacuerdo que la invasión de privacidad, el uso de datos personales sin autorización, la intervención ilegal en las comunicaciones, el espionaje de personas y el uso de información para lograr objetivos en contra de individuos, son prácticas violatorias de los Derechos Humanos?	**El 96%** está de acuerdo.	**El 96%** está de acuerdo.
Comentario: Esta es la pregunta que obtuvo porcentajes más altos de respuesta, coincidiendo en ambos casos.		
12. ¿Usted está de acuerdo o desacuerdo que la vigilancia por medios tecnológicos es una vía para que los gobiernos logren mantener sociedades controladas?	**El 64%** está de acuerdo.	**El 64%** está de acuerdo.
Comentario: Los porcentajes de respuesta también coinciden sin llegas a ser altos. Sólo 6 de cada 10 creen que el espionaje se hace con fines de controlar a las sociedades**.**		
13. ¿Qué tanto considera está haciendo la comunidad internacional para proteger a los ciudadanos del mal uso de la tecnología de espionaje?	**El 72%** opina que muy poco.	**El 68%** opina que muy poco.
Comentario: Las respuestas son muy parecidas, lo que sin duda invita a la comunidad internacional a tomar cartas en el asunto.		

Fuente: Animal Político. 59% de los mexicanos cree que el gobierno los espía: Parametría. [En línea]. https://www.animalpolitico.com/2013/07/59-de-los-mexicanos-cree-que-el-gobierno-los-espia-parametria/. [Página consultada el 26/IX/ 2019].

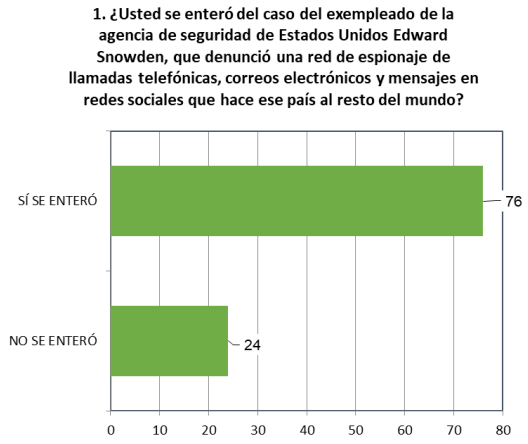
Realizando más análisis, se tiene:

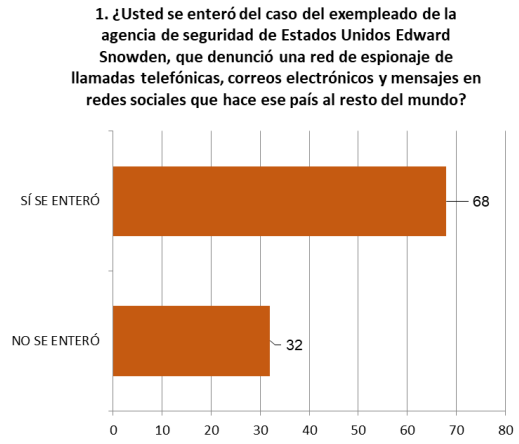
- Como se aprecia, en cinco reactivos se da empate, ello en los cuestionamientos 2, 5, 7, 11 y 12
- En cinco reactivos la diferencia no rebasa el diez por ciento, esto es la 1, 3, 8, 9 y 13
- El mayor contraste se da en la respuesta a la pregunta 10, pues los empleados están de acuerdo en un 52% mientras que los estudiantes están en desacuerdo en el 72%.
- En ningún caso los resultados reflejan puntos extremos.
- En ningún caso alguna respuesta alcanza niveles del 100%.

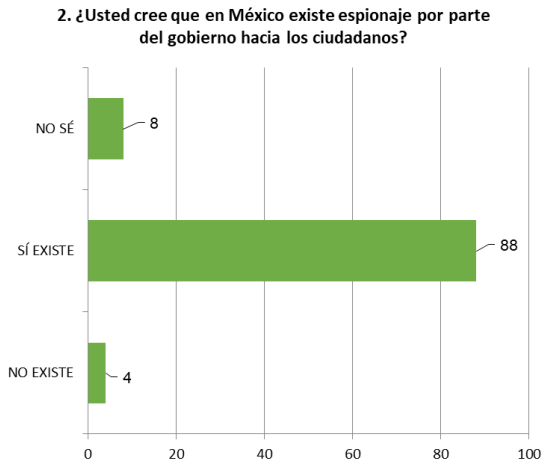
4.5. Gráficas

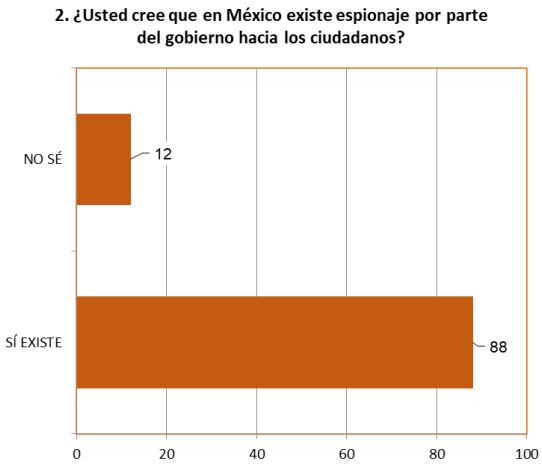
A continuación, se presentan las gráficas para cada cuestionamiento, por separado empleados (verde) y estudiantes (naranja).

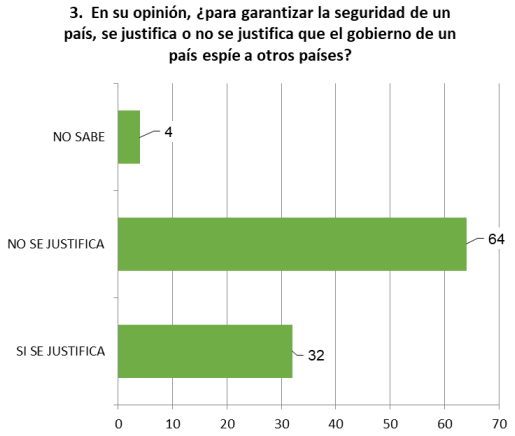
Grafica 2. Preguntas 1-4 de Caso práctico: Preguntas tomadas de: Animal Político

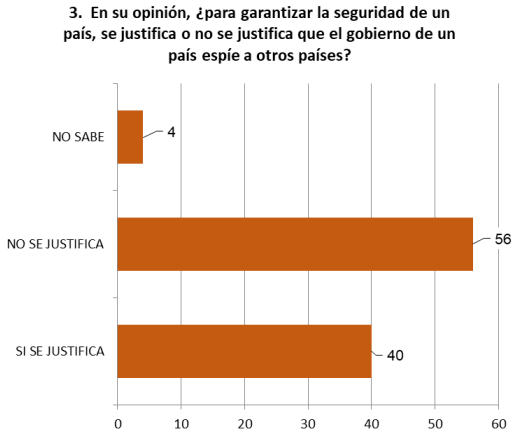


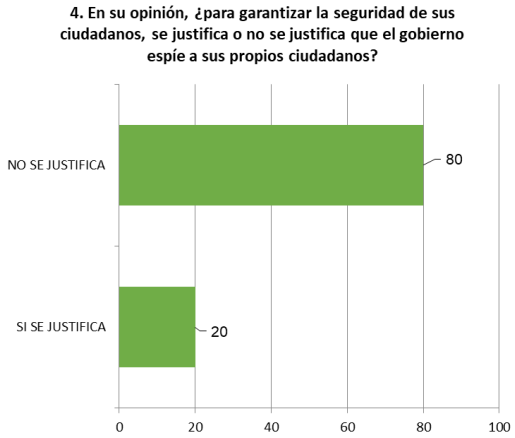


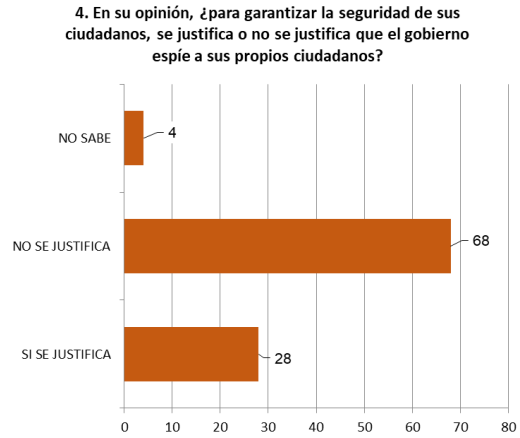






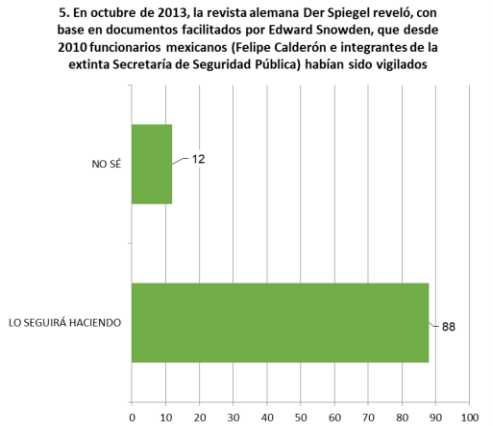


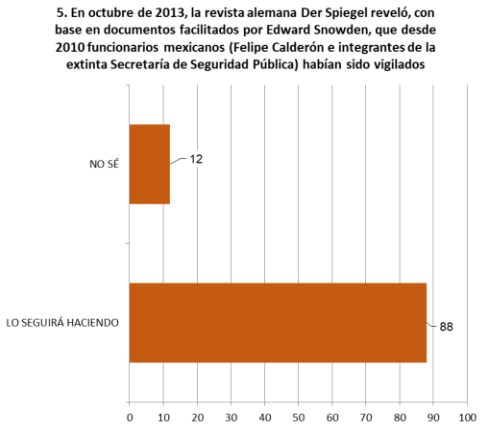


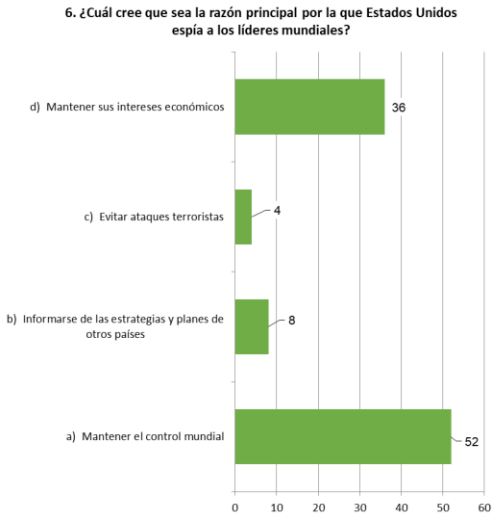


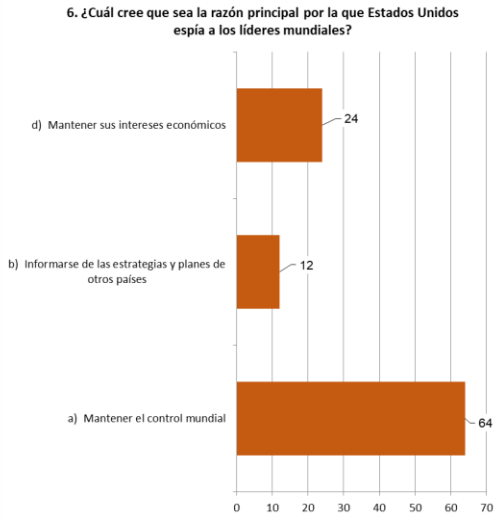
Fuente: Animal Político. 59% de los mexicanos cree que el gobierno los espía: Parametría. [En línea]. https://www.animalpolitico.com/2013/07/59-de-los-mexicanos-cree-que-el-gobierno-los-espia-parametria/. [Página consultada el 26/IX/ 2019].

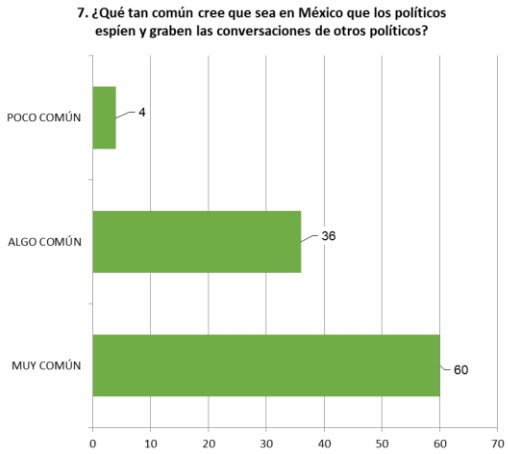
Grafica 3. Preguntas 5-13 de elaboración propia.

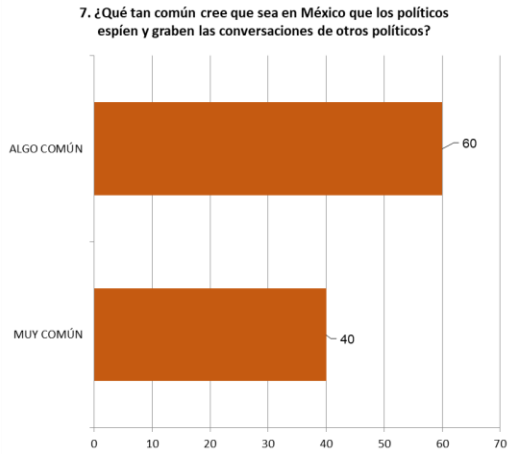


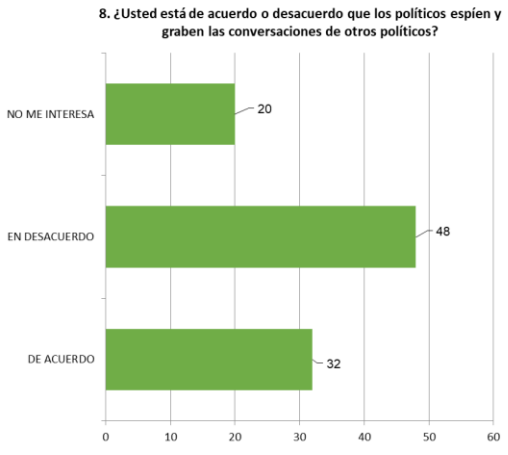


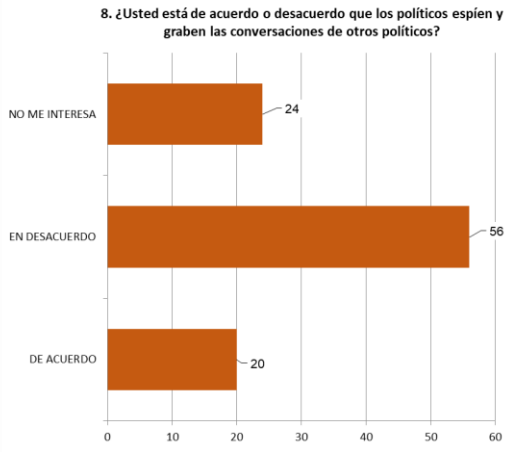

6. ¿Cuál cree que sea la razón principal por la que Estados Unidos espía a los líderes mundiales?
d) Mantener sus intereses económicos
36
c) Evitar ataques terroristas
4
b) Informarse de las estrategias y planes de otros países
8
a) Mantener el control mundial
52
0 10 20 30 40 50 60


6. ¿Cuál cree que sea la razón principal por la que Estados Unidos espía a los líderes mundiales?
d) Mantener sus intereses económicos
24
b) Informarse de las estrategias y planes de otros países
12
a) Mantener el control mundial
64
0 10 20 30 40 50 60 70

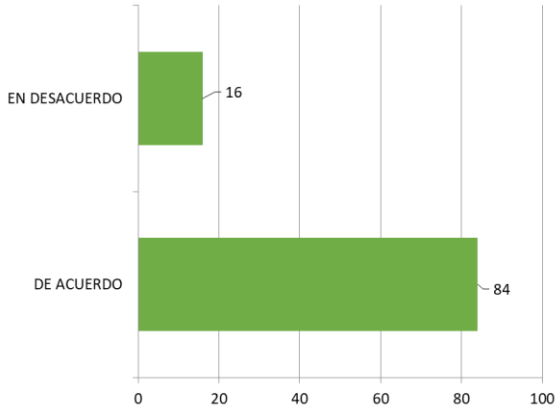

7. ¿Qué tan común cree que sea en México que los políticos espíen y graben las conversaciones de otros políticos?
POCO COMÚN
4
ALGO COMÚN
36
MUY COMÚN
60
0 10 20 30 40 50 60 70


7. ¿Qué tan común cree que sea en México que los políticos espíen y graben las conversaciones de otros políticos?
ALGO COMÚN
60
MUY COMÚN
40
0 10 20 30 40 50 60 70

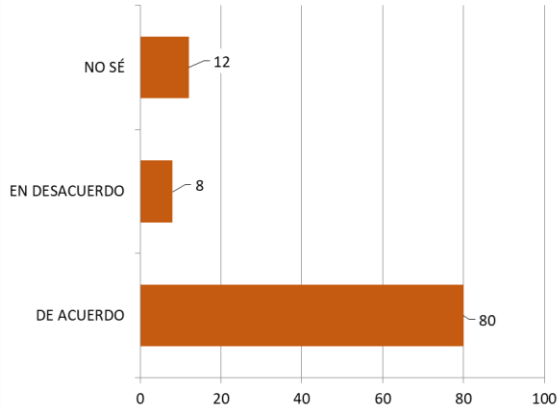

8. ¿Usted está de acuerdo o desacuerdo que los políticos espíen y graben las conversaciones de otros políticos?
NO ME INTERESA
20
EN DESACUERDO
48
DE ACUERDO
32
0 10 20 30 40 50 60


8. ¿Usted está de acuerdo o desacuerdo que los políticos espíen y graben las conversaciones de otros políticos?
NO ME INTERESA
24
EN DESACUERDO
56
DE ACUERDO
20
0 10 20 30 40 50 60

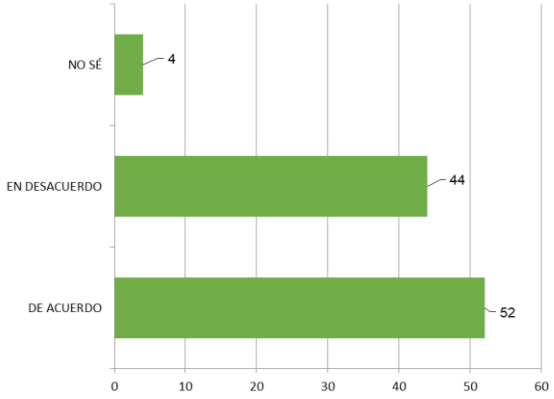
9. ¿Usted está de acuerdo o desacuerdo que el espionaje generalizado mediante el uso de la tecnología es una violación a los Derechos Humanos?



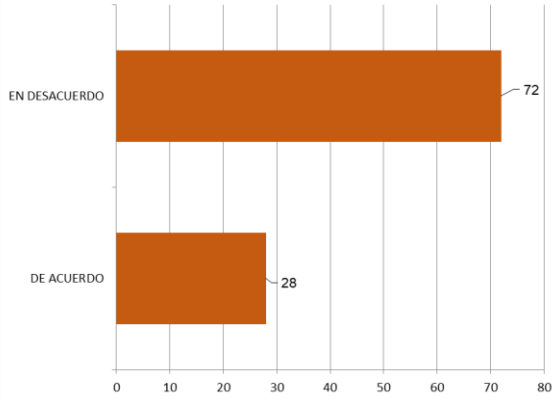
9. ¿Usted está de acuerdo o desacuerdo que el espionaje generalizado mediante el uso de la tecnología es una violación a los Derechos Humanos?



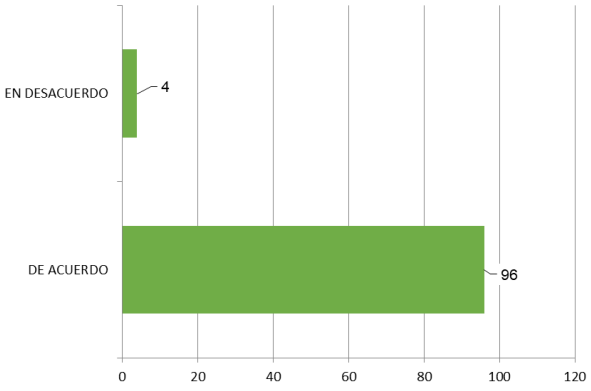
10. ¿Usted está de acuerdo o desacuerdo que a nivel internacional, no exista reglamentación suficiente que proteja los DH de los ciudadanos en contra del uso de la tecnología de espionaje?



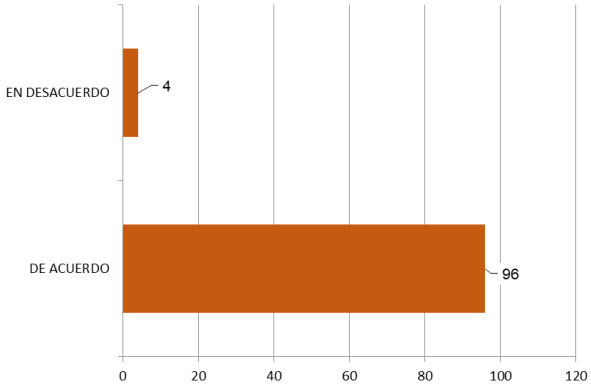
10. ¿Usted está de acuerdo o desacuerdo que a nivel internacional, no exista reglamentación suficiente que proteja los DH de los ciudadanos en contra del uso de la tecnología de espionaje?



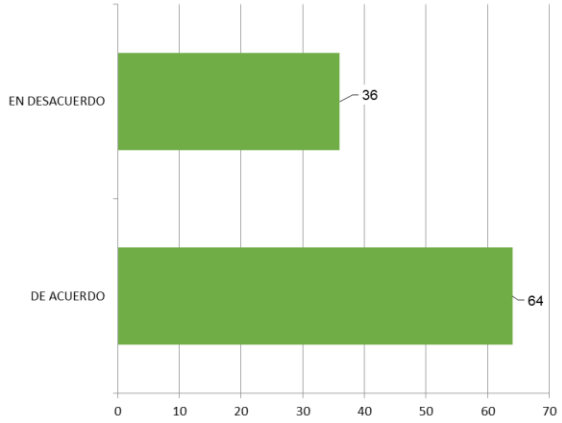
11. ¿Usted está de acuerdo o desacuerdo que la invasión de privacidad, el uso de datos personales sin autorización, la intervención ilegal en las comunicaciones, el espionaje de personas y el uso de información para lograr objetivos en contra de individuo



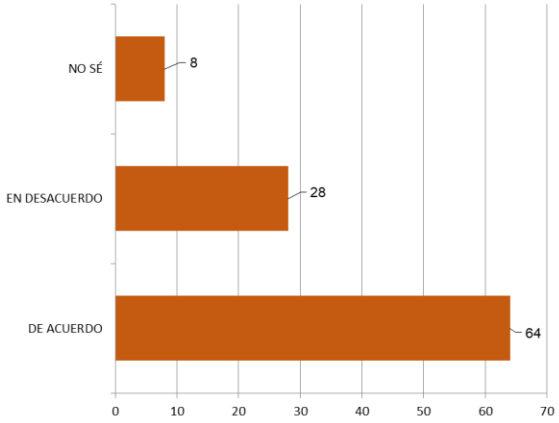
11. ¿Usted está de acuerdo o desacuerdo que la invasión de privacidad, el uso de datos personales sin autorización, la intervención ilegal en las comunicaciones, el espionaje de personas y el uso de información para lograr objetivos en contra de individuo



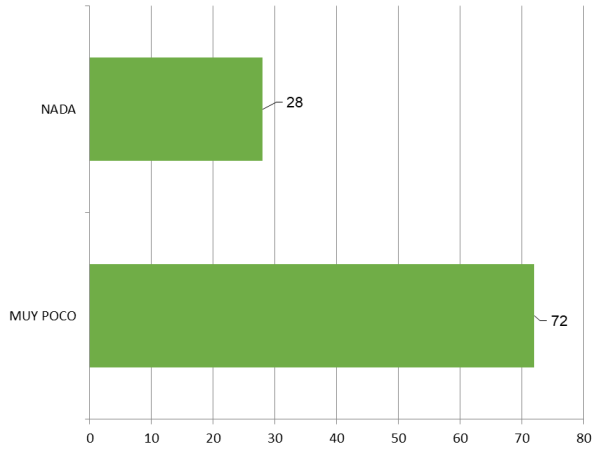
12. ¿Usted está de acuerdo o desacuerdo que la vigilancia por medios tecnológicos es una vía para que los gobiernos logren mantener sociedades controladas?



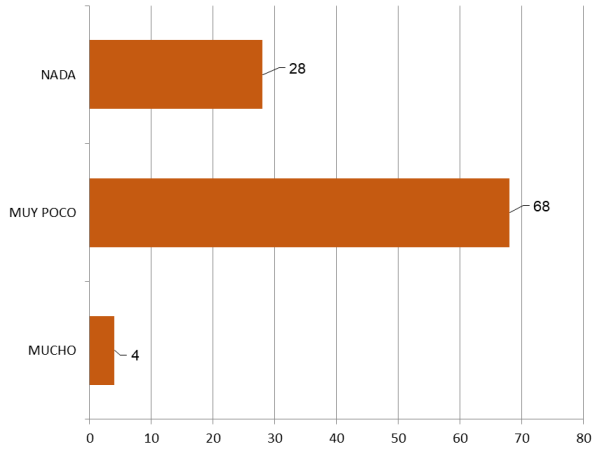
12. ¿Usted está de acuerdo o desacuerdo que la vigilancia por medios tecnológicos es una vía para que los gobiernos logren mantener sociedades controladas?



13. ¿Qué tanto considera está haciendo la comunidad internacional para proteger a los ciudadanos del mal uso de la tecnología de espionaje?

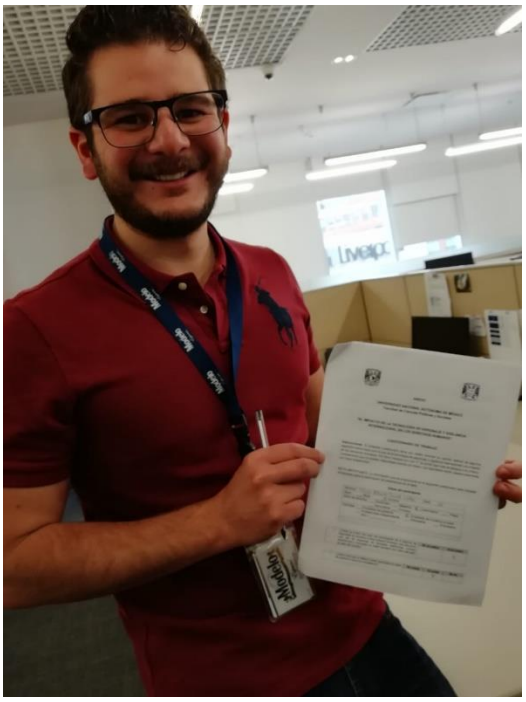


13. ¿Qué tanto considera está haciendo la comunidad internacional para proteger a los ciudadanos del mal uso de la tecnología de espionaje?



4.6. Evidencias de Caso de Estudio

Las personas fotografiadas, otorgaron su permiso para el uso de su persona en el siguiente trabajo.



5. CONCLUSIONES

Con relación al objetivo general planteado al inicio de este trabajo que consiste en analizar el impacto de la tecnología de espionaje y vigilancia internacional y exponer la tensión que se ha provocado entre el orden y el ejercicio de control social, señalando las estructuras de la seguridad a nivel internacional, vislumbrando la relación de poderes con los afectados, como la sociedad civil, organismos no gubernamentales, grupos sociales, y/o periodistas, se informa que este se cumplió positivamente con la realización del trabajo efectuado.

Conocer el proceso de vigilancia basado en el mecanismo de poder.

Una vez que se ha demostrado con información clara y veraz que la tecnología ha sido el impacto más grande para poder vigilar no sólo a la población, sino a naciones enteras, y atendiendo a la hipótesis de trabajo que dicen:

- Hipótesis 1. El espionaje generalizado mediante el uso de la tecnología es una violación a la privacidad internacional. Ya que actualmente, aunque existen instituciones y documentación que protejan a las personas de estos ataques, se ha visto reducido su poder debido a la cantidad de información y con la rapidez con la que es recabada para fines “no legales” pero que pueden afectar en todos los ámbitos a favor de los gobiernos.
- Hipótesis 2. A nivel internacional, no existe reglamentación suficiente que proteja los DD.HH. de los ciudadanos en contra del uso de la tecnología de espionaje tal es el caso de Snowden quién a pesar de contar con las pruebas y el respaldo social, ha sido perseguido hasta hoy día intentando así violentar su estabilidad general mediante amenazas y exilio.
- En esta vía, tampoco existen regulaciones para el uso de dispositivos no reglamentados, tal es el caso de los drones, aparatos que se han visto involucrados ya en distintas circunstancias ilegales y peor aún, de atentados contra el sistema político incluso contra la misma población civil provocando daños colaterales. Y que además son objetos que se encuentran al alcance económico de cualquier persona al no existir una exigencia verdadera sobre el uso de este mecanismo.
- Hipótesis 3. La normalización de las diversas prácticas de vigilancia y/o infiltración han dado lugar a que los Estados cuenten con medios para

mantener sociedades controladas. Por ejemplo: La vigilancia a través de las cámaras de la Ciudad de México, las cuales promueven la seguridad de la ciudadanía y que en efecto se han visto resultados positivos en torno a la delincuencia pero que, a pesar de ello, aún se tiene mucho trecho que recorrer para que su efectividad sea al 100% en pro de la sociedad y no solo en ciertos episodios aislados de éxito. Si bien han sido empleadas para uso benéfico, también han desarrollado experiencias de interrupción de privacidad, autonomía y uso ilegal de la información recabada por las mismas.

Dentro de los hallazgos que dejó la realización del presente trabajo, se tienen los siguientes:

- Se encontró en la investigación, la oportunidad de interesarme en el desarrollo de temas de interés personal, que me siguen invitando a prepararme y desarrollar conocimientos más vastos dentro del ámbito de las Relaciones Internacionales. Además, que el tema abordado medianamente nuevo en el mundo de la investigación y que día con día aumenta la cantidad de información, análisis y problemáticas detectadas, pero, sobre todo, muestras del rumbo hacia donde se está dirigiendo la vigilancia y el espionaje en nuestras vidas, entornos, países y naciones.

Se encontró en esta opción de titulación, un proceso ordenado bajo parámetros de calidad bien establecidos, contando con la acertada orientación de parte de mi asesora.

- Encontré que el análisis de datos es indispensable para aterrizar las inquietudes planteadas. Incluso se implementó el análisis de un pequeño universo de personas mediante una encuesta de solución múltiple en la que se observó no solo la discrepancia con el tema sino también el conocimiento de cómo repercuten en su vida diaria.
- Encontré que el cuerpo de conocimientos de la Licenciatura en Relaciones Internacionales es también a la vez una ciencia y un arte, pues es una disciplina formada por teorías, conceptos, modelos, procesos y herramientas que en su conjunto otorgan valor agregado a las organizaciones, siendo su parte artística, el hacerlas funcionar en las mismas, para que estas sean más eficaces, eficientes y justas.
- Encontré que siempre es necesario ir más allá de la mera investigación ya que a pesar de tener fuentes fidedignas como libros y artículos, siempre es necesario conocer lo que pasa en nuestro entorno, ya que, sin ello, es poco probable tener

una conclusión a un tema real, contemporáneo, vigente y de suma importancia como lo es este.

Las conclusiones de este trabajo de titulación se centran en el logro de los objetivos de la coyuntura del sistema internacional y sus elementos en torno de la vigilancia; concepto que tiene un papel muy importante en la política internacional, ya que países como, por ejemplo, Estados Unidos, juegan un rol determinante en la ejecución de fines que permiten su posición hegemónica.

Las nuevas tecnologías, traen consigo avances que favorecen el tener una mejor calidad de vida, sin embargo, siempre pueden convertirse en una amenaza para la privacidad y la seguridad de la población civil, ya que, mediante ellos, es posible obtener toda la información personal que se requiera para mantener la seguridad nacional o del Estado.

Cabe señalar que, se ha confirmado mediante distintos medios, que Estados Unidos históricamente ha ocupado el espionaje para obtener información de otros países, misma información que en cierto sentido se ha volcado en temas de ventaja e injerencia hacía las naciones; situación que, hasta la fecha, no ha sido aceptada públicamente por dicha nación.

Algunas de las razones por la que justifica el espionaje internacional y basadas en la presente investigación son:

Se confirma que Estados Unidos país que en la investigación representa el mayor porcentaje de casos confirmados y de historia avalada, que actualmente realiza operaciones de espionaje mismas que han levantado a la sociedad, a medios de comunicación y en su mayoría a organizaciones a tener descontento, quejas, y molestias mismas que en muchas ocasiones han sido sofocadas por el mismo gobierno, prueba de ello es la existencia de amenazas a la sociedad civil, asesinatos, desapariciones forzadas y como ya se mencionaba con anterioridad, daño colateral.

En los últimos años, se ha demostrado que Estados Unidos realizó un importante aumento de vigilancia internacional mediante medios tecnológicos a partir de los atentados del 2001, su objetivo primordial era el económico y después del 11S fue la seguridad nacional mismo que reforzó y preservó la misma mediante la implementación de mecanismos y estrategias enfocadas a obtener información que permitan prevenir amenazas o en dado caso, estar preparados para hacerles frente.

Es preocupante que la desinformación en torno a una temática tan acuciante como es la seguridad sea provista por las propias instancias estatales, seguida de medios de

comunicación que alientan el espectáculo de la violencia y los cuerpos de seguridad que con el fin de incrementar sus presupuestos, motiven la desconfianza y el terror dentro de una sociedad, pero que recurren a vigilar sólo a líderes comunitarios o de la opinión pública con el pretexto de vigilar para el ejercicio de las funciones de seguridad pública. Si bien la violencia se sistematiza para consolidar grupos de poder en diversos territorios, no debe ser pretexto para controlar y vigilar por encima de los derechos civiles a la libertad de tránsito y asociación.

Se puede llegar a la conclusión de que, desde hace tiempo y actualmente, el ser humano ha sido y está siempre vigilado, lo cual lo ha llevado a tener una nueva adaptación social ya que, sin este tipo de vigilancia, actualmente la sociedad puede sentirse desprotegida.

Con base en la teoría desarrollada en el trabajo, podemos descifrar que el sistema panóptico del que Bauman nos ha hablado no es un modelo pasado de moda sino por el contrario, es un modelo vigente de vigilancia que analiza y vigila el sistema de poder y control social, ¿Qué pasaría su superamos que las cámaras de la Ciudad de México no sirven? La respuesta es clara, todo tipo de delitos se cometerían ya que no existe un ojo que pueda vigilarte y reconocerte cómo parte de un conjunto inestable frente a la sociedad y cultura.

Por un lado, nos encontramos primero en un punto de poder panóptico en el que el control y la vigilancia fueron desarrollados para tener el orden social de lo que en su momento era la modernidad sólida, es decir la etapa en dónde podemos encontrar mayor sedentarismo ya que los trabajos se realizaban en un mismo lugar.

Por otro lado, en el momento en el que la sociedad se ve alcanzada por una modernidad liquida como la que estamos viviendo ahora, podemos decir que hemos superado de alguna manera la era panóptica ya que está evolucionando la manera de conservar el orden social día con día y es que a partir del desarrollo tecnológico se han encontrado maneras incluyentes para poder controlar, espiar, mover, conmocionar y devastar al mundo y a todos los elementos que trae consigo la nueva internacionalización de la vigilancia.

Si hacemos un recuento histórico, durante la Guerra Fría, se comenzó el uso de ciertos artefactos que servían para realizar operaciones y alcanzar los objetivos sin la necesidad de sacrificar fuerza humana, este es el caso de los drones, los cuales fueron utilizados por Estados Unidos y Rusia para lanzar ataques ocasionando así bajas y daños al enemigo logrando su detección e intención con anticipación.

La vigilancia como tal, juega un papel importante en la política exterior de todo país, ya que la tecnología no solo ha evolucionado la existencia del ser humano, sino que en muchas situaciones maneja un doble uso, por ejemplo, su uso militar y su uso civil que, gracias a los avances, logran mantener un control de forma anónima.

Las telecomunicaciones y el *internet* son mecanismos que presentan un continuo avance y desarrollo, desde un celular y hasta la televisión han afectado la privacidad de la sociedad ya que, a pesar de ser componentes cotidianos de la vida, tienen la capacidad de afectar con el objetivo de transmitir información a los Estados para obtener ventajas sobre la actividad del ciudadano, como los casos de figuras mexicanas que se mencionaron en la investigación.

Es evidente que, las acciones realizadas en torno a la vigilancia y espionaje han afectado a los Derechos Humanos sobrepasando los límites aceptables por cualquier ciudadano. Los gobiernos utilizan medios tecnológicos para obtención de información de manera ilegal ya que, a falta de políticas, normas o reglamentos, es prácticamente operable. A pesar de que existen garantías individuales, estás han puesto en jaque la obtención de información confidencial y personal de la población.

Es cierto que existen múltiples mecanismos jurídicos para mantener la privacidad de la sociedad frente a la Declaración Universal de los Derechos Humanos la cual garantiza la seguridad a la población y garantiza medios de protección para reducir la vulnerabilidad de la vigilancia y el espionaje, sin embargo, estas han sido cuestionadas al no poder garantizar la seguridad que expresan en sus documentos.

El espionaje ha permitido tener ventajas a Estados Unidos posicionándose como el país con mayor influencia e injerencia internacional, lo cual ha provocado una estrategia de política internacional que garantiza evidencia de cualquier peligro a su nación. Gracias a las nuevas herramientas como el uso de *internet*, las redes sociales, y los distintos medios de comunicación, controlar y mantener las bases de datos resulta fácil que se tenga un espionaje desmesurado, surgiendo muy diversas opiniones y reacciones a ello, situación que el Presidente Obama trató de ocultar y que terminó declarando que las relaciones de política exterior seguirían siendo cordiales, de confianza y óptimas para los países involucrados.

Se considera que es necesario tener una actualización continua de las reglamentaciones, tratados y demás sistemas que garanticen la privacidad de cada ciudadano del mundo, se necesita que las políticas sean más claras antes de ser aceptadas por cada usuario además de que los instrumentos y convenios deben ser ampliados para

el beneficio de la población y no como hasta ahora para el beneficio de los gobiernos que han implementado sistemas de vigilancia.

Derivado del trabajo de campo, se utilizó una muestra de 50 personas, 25 estudiantes de la Facultad de Ciencias Políticas y Sociales y otras 25 profesionistas, empleados de empresa pública o privada, se concluye que, en general, la sociedad que conforma a los profesionistas con un trabajo actual, están conscientes e informados de la situación, incluso con algunos se pudo platicar del uso que les dan a sus equipos de cómputo y celulares, vistos como un arma para guardar y clasificar información.

En cambio, el capo estudiantil se encuentra más desinteresado por el tema, en general no les preocupa que actualmente se ejerza una red de espionaje y que sus datos personales puedan ser utilizados para cualquier actividad y en cualquier momento.

Finalmente, con la prueba que se realizó pude obtener información sobre la cantidad de personas que escucharon, leyeron o investigaron algo relacionado con el tema de Snowden o WikiLeaks, actualmente muy pocas personas de la muestra pueden proclamar una postura a favor de Estados Unidos.

Sin duda, actualmente, se vive frente a un panorama de incertidumbre tanto social como político y económico. En teoría, estas tres variables van de la mano para poder llevar a cabo el espionaje o vigilancia que se realiza no solo por parte de Estados Unidos sino también por parte del gobierno mexicano.

Se necesita que existan leyes y regulaciones más justas con la información y la privacidad, que la población se sienta tranquila de poder realizar sus actividades comunes sin pensar en que un dron puede grabarlo mientras corre por las mañanas. Es necesario la creación de nuevas leyes o acuerdos que a nivel internacional tengan reglamentado y justificado el porqué de las acciones locales o gubernamentales y que de eso se dé fe y transparencia al pueblo para poder seguir utilizándolas de una manera responsable.

Creo que como se menciona en el trabajo, los gobiernos están conscientes de la situación de vigilar a las personas mediante el modelo panóptico, modelo que hasta hoy día podemos ver en marcha en cualquier nación o Estado con el fin de mantener bajo un control social a la población, ya sea mediante miedo o psicosis social. Como bien se demuestra en el trabajo, funcionó, funciona y seguirá funcionando mientras no existan leyes y/o regulaciones para el tema.

Para finalizar, considero útil el que cada persona debe tomar conciencia para hacer frente a este tipo de situaciones, como, por ejemplo:

- Revisar los términos y condiciones de cualquier página, sitio, documento o aplicación que se descargue.
- Siempre tener en cuenta la firma y revisión de los términos de privacidad de cada empresa ya que de ello depende que la información social sea utilizada para cualquier otro fin.
- Siempre estar alerta ante cualquier situación de vigilancia.
- Cuidar la información contenida en los aparatos electrónicos.
- Mantener una comunicación fluida con las personas cercanas, es decir, mantener un vínculo en el que se pueda intercambiar información necesaria, principalmente documentación oficial y personal.
- Seguir confiando en las Instituciones, garantías individuales y organizaciones que protegen, cuidan y respaldan la privacidad como un Derecho.

Si bien, el espionaje que se lleva a cabo a través de los nuevos mecanismos de vigilancia no es evidente y mucho menos tangible para el entorno social, aprovechan y es justo bajo esa bandera con la que se desarrollan nuevas actualizaciones y programas día con día, que pueden impactar de manera negativa a ciertos círculos como la seguridad nacional o los Derechos Humanos.

Como sociedad, debemos exigir y tener más información legal para poder distinguir entre este tipo de accesos con conocimientos indebidos de nuestra información, si bien hemos aprendido el contexto de la situación, siempre debemos conocer la parte subjetiva y objetiva de estos nuevos mecanismos y cómo pueden recaer en nuestra situación personal, mundial y en todos los ámbitos posibles con los que podamos hoy o en algún futuro interactuar.

6. Bibliografía

- Arroche Ernesto. *Miedo*. Edit. Article 19. México. 2016. 198 pp.
- Assange Julian. *Cuando google encontró a WikiLeaks.* Capital Intelectual. 2014. Estados Unidos. 235 pp.
- Bauman Zygmunt y David Lyon. *Vigilancia líquida*. Paidós, Barcelona, 176 pp.
- Garland David. *Castigo y Sociedad Moderna*. *Un estudio de Teoría Social*. Siglo Veintiuno Editores. México. 351 pp.
- Garzón-García, David Enrique, Dary Flórez Luz. *Filosofía política: vigencia de la sociedad de control de Michelle Foucault y análisis de la filosofía política de Gilles Deleuze Persona y Bioética*, vol. 15, núm. 2, 2011, Universidad de La Sabana Cundinamarca, Colombia, 208 pp.
- Greenwald Glenn. Snowden. Sin un lugar donde esconderse. Metropolitan Books. 2014. Nueva York. 313 pp.
- Herrera Hermosilla Juan Carlos. Breve historia del espionaje. Ediciones Nowtilus, S.L. Madrid, España, 304 pp.
- Illades Carlos, Teresa Santiago. *Estado de Guerra. De la Guerra Sucia a la Narco Guerra.* Biblioteca Era. 2014. México. 191 pp.
- Keenan Thomas P. *Tecno Siniestro. El lado oscuro de la red: La rendición de la privacidad y la capacitación e la intimidad*. Melusina. 2015. EE.UU. 325 pp.
- Lefébure Antoine. *El caso Snowden. Así espia Estados Unidos al Mundo*. Editorial Capital Intelectual. Argentina. 2014. 362 pp.
- Lozano Jorge. *Secretos en Red*. Madrid. Ediciones Sequitur. 2014. 198 pp.
- Matterlart Armand. *Un mundo vigilado*. Paidos. 2009. Barcelona. 284 pp.
- Mayer Viktor-Schönberger, Kenneth Cukier. *Big Data. La Revolución de los datos masivos.* Turner Editorial. 2013. España. 278 pp.
- Mazzetti Mark. *La Guerra en las sombras*. Crítica. Barcelona, 2013, 311 pp.
- Muñagorri y Juan S. Pegoraro. *Ordenes normativos y control social en Europa y Latinoamérica en la era de la globalización*. Editorial Dykinson. Madrid. 2011. 358 pp.
- Navarro Bonilla D. *Espionaje, seguridad nacional y Relaciones Internacionales*. Colección de Estudios Internacionales. Bilbao, España, 304 pp.
- Orwell George. 1984. Ediciones Leyenda, 2017, México, 221 pp.
- Previsión del volumen de producción de vehículos aéreos no tripulados militares en el mundo de 2015 a 2023. [En línea]. https://es.statista.com/estadisticas/658877/prevision-de-fabricacion-mundial-de-drones-militares/. [Página consultada el 23/VI/2019].
- R. Hernández Sampieri y Lucio Baptista. Metodología de la investigación. Ed. Mc Graw Hill, México, 2006, pp. 715.
- Ramonet Ignacio. *El Imperio de la Vigilancia*. Editorial Clave Intelectual, Madrid, 2015, 167 pp.

- Ricoy Casas, Rosa María. *Algunos ejemplos de espionaje y vulneración de la protección de datos a escala mundial*. Revista de la Escuela Jacobea de Posgrado, Nº 14, 2018, 68 pp.
- Tirado Serrano Francisco y Miguel Domenech i Argemí. *Lo social y lo virtual. Nuevas formas de control y transformación social*. Editorial UOC, México, 2006, 147 pp.
- Whitaker Reg. El fin de la privacidad. Paidós Comunicación, Barcelona, 1999, 238 pp.

7. Ciberografía

- ¿*Cambridge Analytica* opera en México? Esto es lo que se sabe. [En línea]. https://politica.expansion.mx/mexico/2018/03/21/cambridge-analytica-opero-en-mexico-esto-es-lo-que-se-sabe. [Página consultada el 17/VII/2019].
- ¿Pueden las águilas cazar drones? [En línea]. https://www.eulixe.com/articulo/imagen/pueden-las-aguilas-cazar-drones/20190305101351010226.html. [Página consultada el 23/VI/2019].
- ¿Qué es la fuga de información? [En línea]. https://www.bancosantander.es/glosario/fuga-datos. [Página consultada el 24/VI/2021].
- ¿Qué leyes viola el espionaje de la NSA y cómo puedes defenderte? [En línea]. https://hipertextual.com/2013/10/claves-legales-espionaje-nsa. [Página consultada el 06/VI/2019].
- AAI RQ-2A Pioneer — first UAV to accept a military surrender. [En línea]. https://travelforaircraft.wordpress.com/2012/04/20/aai-rq-2a-pioneer-write/. [Página consultada el 05/ VIII/ 2018].
- Acurio Santiago. "Derecho Penal Informático" [En línea]. https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico. [Página consultada el 06/VI/2019].
- Airbus Defence and Space. [En línea]. https://airbusdefenceandspace.com/wp-content/uploads/2016/07/atlante-brochure.pdf. [Página consultada el 10/ VIII/ 2018].
- Animal Político. 59% de los mexicanos cree que el gobierno los espía: Parametría. [En línea]. https://www.animalpolitico.com/2013/07/59-de-los-mexicanos-cree-que-el-gobierno-los-espia-parametria/. [Página consultada el 26/IX/ 2019].
- Aplicaciones Civiles de los Vehículos Aéreos No Tripulados (VANT) / Unmanned Aerial Vehicles (UAV). [En línea]. http://www.aviacioncivil.com.ve/aplicaciones-civiles-de-los-vehiculos-aereos-tripulados-vant-unmanned-aerial-vehicles-uav. [Página consultada el 08/ VIII/ 2018].
- Aristegui Noticias. "La casa blanca de Enrique Peña Nieto". [En línea]. https://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/. [Página consultada el 14/I/2020].

- Aristegui Noticias. La historia que cambió el sexenio. [En línea]. https://aristeguinoticias.com/2403/mexico/la-historia-de-la-casa-que-cambio-la-historia-del-sexenio/. [Página consultada el 14/I/2020].
- Article19, R3D y SOCIAL TIC. Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. 2017. [En línea]. https://r3d.mx/2017/06/19/gobierno-espia/. [Página consultada el 08/ I/ 2018].
- Article19, R3D y SOCIAL TIC. Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. [En línea]. https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf. [Página consultada el 14/I/2020].
- Así fue el caso *WikiLeaks*. [En línea]. https://www.elperiodico.com/es/internacional/20170118/asi-fue-el-caso-*WikiLeaks*-5750289. [Página consultada el 09/ II/ 2019].
- AZ Noticias. Presidencia de México niega espionaje del que se le acusa. [En línea]. https://aznoticias.mx/index.php/mexico-movil/23868-presidencia-de-mexico-niega-el-espionaje-del-que-se-le-acusa [Página consultada el 26/VII/ 2019].
- Barranco Fragoso Ricardo. IBM. Developer Works. "¿Qué es *Big Data*?" [En línea]. https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/. [Página consultada el 10/ II/ 2018].
- BBC News. 5 claves para entender el escándalo de *Cambridge Analytica* que hizo que Facebook perdiera US$37.000 millones en un día. [En línea]. https://www.bbc.com/mundo/noticias-43472797 [Página consultada el 18/VII/2019].
- *Big Data* Future. Los Small Data: La última milla del *Big Data*. [En línea]. https://bigdata400.wordpress.com/ [Página consultada el 24/VI/2019].
- *Big Data* Future. Los Small Data: La última milla del *Big Data*. [En línea]. https://bigdata400.wordpress.com/ [Página consultada el 24/VI/2019].
- Bracero Francesc. "Aplicaciones de espionaje". [En línea]. https://www.ucm.es/data/cont/media/www/pag-48257/UOC.pdf. [Página consultada el 09/ I/ 2018].
- Calveiro Pilar. Violencias de Estado. "La Guerra antiterrorista y la Guerra contra el crimen como medios de control global". [En línea]. file:///C:/Users/Laura%20Gonzalez/Downloads/37-71-1-SM.pdf. [Página consultada el 08/ I/ 2018].
- Cámara de Diputados del H. Congreso de la Unión. "Ley de Seguridad Nacional". [En línea]. http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf. [Página consultada el 05/VI/2019].
- Casos como *Pegasus* demuestran necesidad de tener MPS y Fiscalía Autónomos: Pardinas. [En línea]. https://aristeguinoticias.com/2905/mexico/casos-como-*Pegasus*-demuestran-necesidad-de-tener-mps-y-fiscalia-autonomos-pardinas/. [Página consultada el 20/VII/2019].
- Castells Manuel. "Vivir en un estado de vigilancia permanente" https://ssociologos.com/2015/03/12/vivir-en-estado-de-vigilancia-permanente-manuel-castells/. [Página consultada el 08/ I/ 2019].

- Celag.org. “Cambridge Analytica, *Big Data* y su influencia en las elecciones” [En línea]. https://www.celag.org/cambridge-analytica-el-big-data-y-su-influencia-en-las-elecciones/. 43472797 [Página consultada el 17/VII/2019].
- Central Intelligence Agency US. “Acerca de la CIA”. [En línea]. https://www.cia.gov/es. [Página consultada el 08/ XI/ 2018].
- CNDH. “Comunicado de Prensa DGC/203/17”. [En línea]. http://www.cndh.org.mx/sites/all/doc/Comunicados/2017/Com_2017_203.pdf. [Página consultada el 29/V/2019].
- Curzio L. La seguridad nacional en México. [En línea]. http://www.cisan.unam.mx/pdf/lc02_04.pdf. [Página consultada el 21/VI/2019].
- De Alva Volnié Eduardo, Meléndez Flores Jorge Emilio “Espionaje en estados unidos: descubriendo la historia secreta”. [En línea]. http://vinculacion.dgire.unam.mx/Congreso-Trabajos-pagina/PDF/Congreso%20Estudiantil%202014/Proyectos%202014-%20%C3%81rea/5.%20%C3%81reas%20de%20Convergencia/1.9%20CIN2014A50109-%20Literatura.pdf. [Página consultada el 10/ I/ 2018].
- Deleuze Gilles. Post-scriptum sobre las sociedades de control Polis, Revista de la Universidad Bolivariana, vol. 5, núm. 13, 2006, Universidad de Los Lagos Santiago, Chile. [En línea]. https://journals.openedition.org/polis/5509. [Página consultada el 08/ I/ 2018].
- Deloitte. “Sin autorización judicial, espiar es un acto ilegal”. [En línea]. https://www2.deloitte.com/mx/es/pages/dnoticias/articles/actividades-de-espionaje.html. [Página consultada el 09/ XII/ 2019].
- Detectan en México tres operadores activos del *software* espía *Pegasus*. [En línea]. https://aristeguinoticias.com/2009/mexico/detectan-en-mexico-tres-operadores-activos-del-*software*-espia-*Pegasus*/. [Página consultada el 09/XI/ 2018].
- Diario Turing. Galldon Clavell Gemma. “Espionaje y derechos humanos: los límites a la intromisión de la intimidad”. [En línea]. https://www.eldiario.es/turing/Espionaje-derechos-humanos_0_159934512.html. [Página consultada el 02/VI/2019].
- Diego Navarro Bonilla. Espionaje, seguridad nacional y Relaciones Internacionales. [En línea]. https://web-argitalpena.adm.ehu.es/pdf/USPDF170933.pdf. [Página consultada el 21/VI/2019].
- Directory of U.S. Military Rockets and Missiles. [En línea]. http://www.designation-systems.info/dusrm/m-105.html. [Página consultada el 019/ III/ 2019].
- Dominique Foray. La sociedad del conocimiento. Revista internacional de ciencias sociales, marzo, 2002, No. 171. [En línea] http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/171-abstracts171spa.pdf. [Página consultada el 16/ I/ 2018].
- Drones estadounidenses. Drones más pequeños y con menos capacidades para el futuro cercano. [En línea]. https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Cuarto-Trimestre-2018/Drones-estadounidenses/. [Página consultada el 09/ II/ 2019].

- Echelon. La red de espionaje planetario. [En línea]. http://www.melusina.com/rcs_gene/0068-e_echelon.pdf [Página consultada el 18/VII/2019].
- Eggen, Dan. “Washington Post. Bush Authorized Domestic Spying”. [En línea]. http://www.washingtonpost.com/wpdyn/content/article/2005/12/16/AR2005121600021.html. [Página consultada el 29/ XI/ 2018].
- El arma de moda: Impacto del uso de los drones en las Relaciones Internacionales y el Derecho Internacional Contemporáneo. [En línea]. Dirección URL: http://icip.gencat.cat/web/.content/continguts/publicacions/arxius_icip_research/ICIP_RESEARCH-4_WEB.pdf [Página. consultada el 27/I/2018].
- El Heraldo de México. Espionaje y futuro del CISEN. En línea]. https://heraldodemexico.com.mx/opinion/espionaje-y-futuro-del-cisen/ [Página consultada el 26/VII/ 2019].
- El Universal Internacional. “Estados Unidos invierte $53.000 millones en espionaje.31 de agosto de 2013”. [En línea]. http://www.eluniversal.com/internacional/130831/EE.UU.invierte-53000-millones-en-espionaje. [Página consultada el 29/ XI/ 2018].
- El Universal. “Espionaje: grave violación a los derechos humanos”. [En línea]. http://www.eluniversal.com.mx/entradadeopinion/articulo/markocortes/nacion/2017/07/11/espionaje-grave-violacion-los-derechos. [Página consultada el 29/V/2019].
- Espionaje y seguridad en las redes. [En línea]. https://es.slideshare.net/LauDiaz05/espionaje-y-seguridad-en-las-redes. [Página consultada el 08/III/2021].
- E-uaem. *Selección de la muestra.* [En línea]. http://euaem1.uaem.mx/bitstream/handle/123456789/2776/506_6.pdf?sequence=1&isAllowed=y. [Página consultada el 26/I/ 2020].
- Expansión. “Casi un millón de mexicanos afectados por Cambridge Analytica”. [En línea]. https://expansion.mx/tecnologia/2018/04/04/casi-un-millon-de-mexicanos-afectados-por-cambridge-analytica. [Página consultada el 18/VII/2019
- Fayer Wayer. Segundo día: puntos clave sobre la declaración de Mark Zuckerberg ante el Congreso. [En línea]. https://www.fayerwayer.com/2018/04/segundo-dia-puntos-clave-zuckerberg/ [Página consultada el 09/VII/2019].
- Fernández-Carrión Miguel Héctor. Control social en la sociedad de red. Nóesis. Revista de Ciencias Sociales y Humanidades. México. 2007. [En línea]. https://dialnet.unirioja.es/servlet/articulo?codigo=2265397. [Página consultada el14/XII/ 2018].
- First cruise missile- Kettering´s Bug. [En línea]. https://travelforaircraft.wordpress.com/2011/04/01/first-cruise-missile-%E2%80%94-the-kettering-bug/. [Página consultada el 03/ VIII/ 2018].
- Forbes. *Cambridge Analytica* sí capturó datos personales en México: exdirectora. [En línea]. https://www.forbes.com.mx/cambridge-analytica-si-capturo-datos-personales-en-mexico-ex-directora/ [Página consultada el 09/VII/2019].

- Foreign relations of the United States, 1945–1950, emergence of the Intelligence establishment. [En línea]. https://history.state.gov/historicaldocuments/frus1945-50Intel/d160. [Página consultada el 13/ XII/ 2018].
- Gaceta del Senado. [En línea]. https://www.senado.gob.mx/64/gaceta_del_senado/documento/81027. [Página consultada el 09/ XI/ 2019].
- Gaceta Oficial de la República Bolivariana de Venezuela Ley Especial contra los "Delitos Informáticos". [En línea]. https://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf. [Página consultada el 05/VI/2019].
- Gobierno Espía: La vigilancia sistemática en contra de los periodistas y defensores de Derechos Humanos en México. [En línea]. https://imco.org.mx/wp-content/uploads/2017/06/Comunicado_Orgs.pd. [Página consultada el 09/XI/ 2018].
- Greenwald, Glenn. Sin un lugar donde esconderse. [En línea]. https://reexistencia.files.wordpress.com/2011/02/snowden-completo.pdf [Página consultada el 08/VII/2019].
- Hipertextual. Cronología del caso Snowden, el hombre más buscado del mundo. [En línea]. https://hipertextual.com/2016/03/cronologia-edward-snowden [Página consultada el 08/VII/ 2019].
- Josep Albors. ¿Sabes que es un exploit y cómo funciona? [En línea]. https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/. [Página consultada el 12/VII/2019].
- Juagaribe Helio. "El Vietnam y los Estados Unidos". Instituto de Estudios Internacionales Universidad de Chile. Chile. [En línea]. file:///C:/Users/Karla%20SG/Downloads/17324-1-56255-1-10-20120409.pdf. Pp. 12. [Página consultada el18/XII/ 2018]
- KGB. [En línea]. https://actualidad.rt.com/actualidad/258012-rusia-celebrar-centenario-organos-seguridad-nacional. [Página consultada el 15/ XI/ 2018].
- La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EE.UU. 2013. [En línea]. https://www.files.ethz.ch/isn/174181/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf. [Página consultada el18/XII/ 2018].
- La NSA, según las revelaciones de Snowden. [En línea]. http://www.rebelion.org/docs/234497.pdf. [Página consultada el 09/XI/ 2019].
- La Red Echelon: la gran oreja. [En línea]. https://www.bibliotecapleyades.net/ciencia/echelon02.htm [Página consultada el 15/VII/2019].
- La Sociedad de control. Una mirada al S. XXI desde Foucault. [En línea]. https://www.scielo.cl/scielo.php?pid=S0718-43602017000100317&script=sci_abstract. [Página consultada el 21/VI/2020].
- Las 5 V y que sirven para explicar el *Big Data*. [En línea]. https://www.master-bigdata.com/big-data-5-v/#:~:text=La%20veracidad%20puede%20entenderse%20como,la%20confianza%20en%20los%20mismos. [Página consultada el 24/VI/2020].

- Las 5 vs que caracterizan el concepto de *Big Data*. [En línea]. https://www.vision*software*.com.co/las-5-vs-que-caracterizan-el-concepto-de-big-data/. [Página consultada el 24/VI/2020].
- Legislación en diferentes países sobre los delitos informáticos [En línea]. https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm. [Página consultada el 06/VI/2019].
- Ley Patriotica de los Estados Unidos. United States Interametican Community Affairs. [En línea]. http://interamerican-usa.com/articulos/Leyes/US-Patriot%20Act.htm. [Página consultada el 15/ XII/ 2018].
- Liberta Bonilla, B.E. (2007) "Impacto, impacto social y evaluación del impacto. Acimed". [En línea]. http://scielo.sld.cu/pdf/aci/v15n3/aci08307.pdf [Página consultada el 22/V/ 2019].
- Los Drones y sus aplicaciones en la Ingeniería Civil. Madrid. [En línea] http://www.fenercom.com/pdf/publicaciones/Los-Drones-y-sus-aplicaciones-a-la-ingenieria-civil-fenercom-2015.pdf. [Página consultada el 04/ II/ 2018].
- Maldonado Guanota, Alexandra. Herramientas para evitar la infiltración y penetración en el ejército de Colombia. [En línea]. http://repository.unimilitar.edu.co/bitstream/10654/7540/1/GuanotoaMaldonadoAlexandra201 2.pdf. [Página consultada el 09/I/ 2018].
- Michael Choussudovsky. Línea de Fuego. "Quién está detrás de *WikiLeaks*? 2011. [En línea]. https://lalineadefuego.info/2011/01/25/%C2%BFquien-esta-detras-de-*WikiLeaks*-michel-chossudovsky/. [Página consultada el18/XII/ 2018].
- Milenio Noticias. ¿Qué es *Pegasus*? El *malware* para espiar a México. [En línea]. http://www.milenio.com/estilo/que-es-*Pegasus*-el-*malware*-usado-para-espiar-en-mexico. [Página consultada el 09/XI/ 2018].
- Necessary & proportionate. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. [En línea]. https://necessaryandproportionate.org/es/text. [Página consultada el 05/VI/2019].
- Noticias sobre seguridad de la información. Operación Aurora, exfiltró información de espionaje desde Google. [En línea]. https://blog.segu-info.com.ar/2013/05/operacion-aurora-exfiltro-informacion.html. [Página consultada el 14/VII/2019].
- Obama explica por qué Estados Unidos no puede perdonar a Snowden. [En línea]. https://www.genbeta.com/actualidad/obama-explica-por-que-estados-unidos-no-puede-perdonar-a-snowden. [Página consultada el 09/ IX/ 2018].
- Operación Aurora. El ataque hacker mejor planeado de los tiempos. [En línea]. https://si3h-c5ir7.blogspot.com/2011/09/operacion-aurora-el-ataque-hacker-mejor.html [Página consultada el 08/VII/2019].
- Ornelas Bernal, Raúl. Un mundo nos espía. El escándalo ECHELON [En línea]. http://let.iiec.unam.mx/sites/let.iiec.unam.mx/files/OrnelasEchelonChiapas9.pdf [Página consultada el 08/VII/2019].
- Oscar Álvarez Araya. [En línea]. https://wsimag.com/es/cultura/62465-chanakya-el-maquiavelo-de-la-india. [Página consultada el 29/V/2019].

- Palacios Barrera, H; Díaz Ibáñez, E. La seguridad en el Caribe. retos, desafíos y amenazas para la integración Ciencia en su PC, núm. 3, 2008, Centro de Información y Gestión Tecnológica de Santiago de Cuba Santiago de Cuba, Cuba, pp. 96-107
- Paños Antonio. “Influencia de las tecnologías de la información en los procesos de información y toma de decisiones de las empresas”. Facultad de Ciencias de la Documentación. Universidad de Murcia. [En línea]. http://pendientedemigracion.ucm.es/info/multidoc/multidoc/revista/num10/paginas/pdfs/Apan os.pdf. [Página consultada el 6/ XII/ 2018].
- *Pegasus* la impresionante herramienta de espionaje se utilizó contra un periodista en México. [En línea]. https://www.xataka.com.mx/otros-1/*Pegasus*-la-impresionante-herramienta-de-espionaje-se-utilizo-contra-un-periodista-en-mexico. [Página consultada el 20/VII/2019].
- *Pegasus*, el mayor spyware de móviles, ha infectado a Iphone y Android en 45 países. [En línea]. https://www.adslzone.net/2018/09/18/*Pegasus*-spyware-nso-group/. [Página consultada el 09/ XI/ 2018].
- Presentan "dron ambulancia" capaz de transportar desfibrilador. [En línea]. https://www.telemetro.com/tecnologia/2014/10/28/presentan-prototipo-ambulancia-transportar-desfibrilador/1682396.html. [Página consultada el 25/VI/2019].
- Procesamiento masivo de datos: volumen, variedad y velocidad, magnitudes y nuevos retos del *Big Data*. [En línea] https://blog.es.logicalis.com/analytics/velocidad-variedad-y-volumen-las-3-magnitudes-clave-de-big-data. [Página consultada el 24/VI/2020].
- Procesamiento masivo de datos: volumen, variedad y velocidad, magnitudes y nuevos retos del *Big Data*. [En línea] https://blog.es.logicalis.com/analytics/velocidad-variedad-y-volumen-las-3-magnitudes-clave-de-big-data. [Página consultada el 24/VI/2020].
- Proceso. “¿De qué más es capaz, presidente siniestro?: Aristegui”. En línea]. https://www.proceso.com.mx/491688/capaz-presidente-siniestro-aristegui [Página consultada el 27/VII/ 2019].
- Proceso. “Espionaje viola los derechos humanos, hay que investigarlo: CNDH”. [En línea]. https://www.proceso.com.mx/410887/espionaje-viola-los-derechos-humanos-cndh. [Página consultada el 29/V/2019].
- Proceso. Cambridge Analytica: el poder de la desinformación. [En línea]. https://www.proceso.com.mx/527974/cambridge-analytica-el-poder-de-la-desinformacion [Página consultada el 19/VII/2019].
- Pulido Cabañete Estrella. “*Big Data* ¿Solución o problema?”. [En línea]. http://arantxa.ii.uam.es/~epulido/bigdata.pdf. [Página consultada el 08/ I/ 2018].
- R3D. “¿Quién no defiende tus datos? 2018” [En línea]. p.21https://r3d.mx/wp-content/uploads/R3D-QNDTD_digital.pdf. [Página consultada el 03/VI/2019].
- Ramón Tijeras. Comunicación 21. *WikiLeaks*, el periodismo tradicional y las nuevas plataformas de información. [En línea]. http://www.comunicacion21.com/de-*WikiLeaks*-a-openleaks-la-crisis-de-los-medios-y-las-nuevas-plataformas-de-informacion/. [Página consultada el 08/ I/ 2018].

- Rebeca María Calderón Canales,Vilma Consuelo Chiquillo Benítez, Yasmin Elizabeth Rodríguez Peña. “El espionaje como instrumento de la política exterior de Estados Unidos de América y las consecuencias en sus Relaciones Exteriores. casos: República federal de Alemania y República Rederativa de Rrasil. Reriodo 2011-2014”. [En línea]. http://ri.ues.edu.sv/8260/1/UES.%20RELACIONES%20INTERNACIONALES.%20TRABAJO%20DE%20GRADUACION.pdf. [Página consultada el 10/ I/ 2018].
- Red de Defensa de los Derechos Digitales. [En línea]. https://r3d.mx/privacidad/. [Página consultada el 02/VI/2019].
- Red Rompe el Miedo. “Elecciones 2018” [En línea]. https://r3d.mx/wp-content/uploads/RRM-2018.pdf. [Página consultada el 03/VI/2019].
- Ricardo García Jimenez. *El Panoptismo. Nuevas formas de control social*. [En línea]. https://www.eumed.net/rev/cccss/06/rgj2.htm. [Página consultada el18/XII/ 2019].
- Rise of the Reapers: A brief history of Drones. [En línea]. https://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones/. [Página consultada el 03/ VIII/ 2018].
- Rodríguez Pablo Esteban. “¿Qué son las sociedades de control?”. [En línea]. http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf. [Página consultada el 08/ I/ 2018].
- SA surveillance programs live on, in case you hadn't noticed”. [En línea]. https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/. [Página consultada el 09/ IX/ 2018].
- Secretaría de la Función Pública. [En línea]. http://pcop.funcionpublica.gob.mx/index.php/conoce-la-sfp.html. [Página consultada el 09/ XII/ 2019].
- Sepúlveda Whittle, T. (1936). “Espionaje y Contra-Espionaje”. [En línea]. http://agenciabk.net/espionajecontra.pdf. (p.9). [Página consultada el 20/V/2019].
- Shoshana Zuboff. La era del capitalismo de vigilancia. [En línea]. https://planetadelibroscom.cdnstatics2.com/libros_contenido_extra/45/44333_La_era_del_capitalismo_de_la_vigilancia.pdf. [Página consultada el 21/V/2021].
- Siprnet: where America stores its secret cables. The Guardian. [En línea]. https://www.theguardian.com/world/2010/nov/28/siprnet-america-stores-secret-cables. [Página consultada el 28/ XII/ 2018].
- Space.com. What is a Drone. Howell, Elizabeth. [En línea]. http://www.space.com/29544-what-is-a-drone.html. [Página consultada el 09/ II/ 2018].
- Tarragona, Laia. “El Estado de derecho frente al estado espía”. CIDOB. Investigadora CIDOB. 2013. Opinión CIDOB. [En línea]. http://www.cidob.org/es/publicaciones/opinion/seguridad_y_politica_mundial/el_estado_de_d erecho_frente_al_estado_espia. [Página consultada el 29/ XI/ 2018].
- Te sorprendería saber lo que Facebook sabe de ti. Washington. [En línea]. https://www.elimparcial.com/EdicionEnLinea/Notas/Internacional/25032018/1321015-Te-sorprenderia-saber-todo-lo-que-Facebook-sabe-de-ti.html. [Página consultada el 09/ IX/ 2018].

- *The Aviation Wing.* [En línea]. https://www.theaviationwing.com/ryan-firebee/. [Página consultada el 019/ III/ 2019].
- *The Curtiss Company*. [En línea]. https://www.centennialofflight.net/essay/Aerospace/Curtiss/Aero2.htm [Página consultada el 019/ III/ 2019].
- The Free Dictionary. "Espionaje definición". [En línea]. http://es.thefreedictionary.com/espionaje [Página consultada el 08/ XI/ 2018]
- The New York Times. "Somos los nuevos enemigos del Estado: el espionaje a activistas y periodistas en México". [En línea]. https://www.nytimes.com/es/2017/06/19/espanol/america-latina/mexico-*Pegasus*-nso-group-espionaje.html. [Página consultada el 26/VII/ 2019].
- The New York Times. "Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México". [En línea]. https://www.nytimes.com/es/2017/06/19/mexico-*Pegasus*-nso-group-espionaje/. [Página consultada el 30/V/2019].
- The radioplane OQ-2 aereal targer drone was the first quantitaive UAV purchase for the Unitad States. Military Factory. [En línea]. http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=331. [Página consultada el 019/ II/ 2019].
- Torres Apablaza, I. Inflexiones Foucalteanas sobre la sociedad de control. Chile. [En línea]. http://www.redalyc.org/pdf/396/39643561011.pdf. [Página consultada el 09/ IX/ 2018].
- V1 Reichenberg. [En línea]. http://www.v1-reichenberg.com/geschichte_d.html. [Página consultada el 04/ VIII/ 2018].
- Valdivieso P. Jarabo. (2015). El Espionaje. Pasado y Presente. [En línea]. https://apavaldeluz.files.wordpress.com/2015/05/el-espionaje-pablo-jarabodef.pdf. [Página consultada el 29/V/2019].
- Velázquez Olivera, A. El mundo de los drones. [En línea]. www.cienciorama.unam.mx/a/pdf/538_cienciorama.pdf. [Página consultada el 23/VI/2019].
- Vizio podría atajar la recogida indebida de datos. [En línea]. https://www.xatakahome.com/televisores/vizio-podria-atajar-recogida-indebida-datos-ofreciendo-notificacion-pantalla-a-usuarios-afectados. [Página consultada el 09/ IX/ 2018].
- *WikiLeaks*. Collateral Murder. [En línea]. https://www.youtube.com/watch?v=teCB48QT1zs. [Página consultada el 12/ I/ 2018].
- Wordpress. "Espionage during the Cold War". [En línea]. http://istihbaratdunyasi.files.wordpress.com/2012/05/espionage-during-the.pdf. [Página consultada el 12/XI/ 2018].