La vigilancia internacional en el Siglo XXI y el rol del Estado: el caso del programa PRISM en Estados Unidos.

Sabina Dematté

4468213-5

sabb.dematte@hotmail.com

Monografía Final de Investigación de Grado en Relaciones Internacionales

Tutora: Mag. Mónica Nieves

2019

Facultad de Derecho

Universidad de la República

Índice

Resumen

Esta investigación se centra en la vigilancia internacional ejercida por las corporaciones internacionales, y el rol del Estado teniendo en cuenta que la vigilancia es uno de los atributos soberanos de los Estados. El foco se encuentra en las revelaciones de Edward Snowden sobre el programa PRISM, para ejemplificar el alcance de las corporaciones internacionales en materia de vigilancia y las diversas alianzas que se configuran a partir del programa.

Analizando distintos materiales bibliográficos se busca describir la influencia en los ejercicios de los atributos soberanos del Estado de la capacidad de vigilancia internacional de las corporaciones privadas, conocidas mundialmente a través de las mencionadas revelaciones de Edward Snowden.

Palabras clave: Vigilancia – Ciberseguridad – Internet – Estado – Soberanía

INTRODUCCIÓN

Presentación del tema

En el año 2013, *The Guardian* (Inglaterra) y luego varios medios de prensa en Estados Unidos revelaron la noticia sobre un programa secreto de Estados Unidos, más específicamente de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) (Poitras, 2014).

El programa llevaba a cabo la vigilancia masiva de todos los ciudadanos, no solo de Estados Unidos, sino que también del mundo. Estas revelaciones fueron hechas al periodista Glenn Greenwald y la cineasta Laura Poitras, por parte de Edward Snowden.

Edward Snowden había trabajado dentro de la NSA, pero a través de la contratista *Booz Allen Hamilton*, una empresa de tecnología que hace consultoría y análisis. De esta empresa fue extraída la información mediante una tarjeta de memoria que Edward Snowden ingresó a la empresa con el objetivo de extraer dicha información y presentarla a la prensa para su publicación, y que se hiciera de conocimiento público.

Considerando que uno de los atributos soberanos del Estado es el de la vigilancia (Ibarra, Nieves, 2016) con el fin de mantener la seguridad en el territorio, lo novedoso del programa (Greenwald, 2014) es la participación de grandes corporaciones privadas, que pese a que el programa está dirigido por la NSA, es decir por una agencia dentro del gobierno de Estados Unidos, la información proviene de estas corporaciones, así como de alianzas con otros Estados.

Otra novedad del programa es su alcance (Greenwald, 2014), los atributos soberanos de los Estados se ejercen dentro de su territorio, sin embargo el alcance del programa *PRISM*, en concreto, es global, y busca que nada quede por fuera de él mismo.

Delimitación del objeto de estudio

El objeto de estudio es la vigilancia internacional en función del Estado soberano, no obstante el de vigilancia es un concepto muy amplio para ser definido para esta investigación en particular. La vigilancia internacional es tomada en este caso como los métodos y mecanismos que tienen diversas compañías con alcance internacional para acceder a información de sus usuarios y compartirla como herramienta de clasificación y

control de los ciudadanos por parte del gobierno de Estados Unidos como por otros que puedan acceder a dicha información.

El alcance del acceso a la información de los usuarios por parte de las compañías es tomado de las develaciones de Edward Snowden sobre el programa PRISM, que se hizo de público conocimiento en 2013 (Greenwald, 2014). Es decir, que el periodo de análisis está limitado a ese año. No obstante, dentro del concepto vigilancia internacional en ciertas ocasiones se mencionaran también divulgaciones de operaciones del gobierno sobre espionaje como las brindadas por la organización Wikileaks[1], en funcionamiento desde el 2006. Es necesario incluirlas principalmente a modo de ejemplo acerca de la escala del tema, y del poder que se tiene manejando información derivada de la vigilancia internacional.

Por lo tanto, se puede acotar el análisis a realizar sobre la vigilancia internacional dentro del año 2013, y solamente abordándola desde el programa *PRISM*.

También sin perjuicio de mencionar el espionaje realizado a partir del gobierno de Estados Unidos, se enmarca principalmente en la vigilancia que ejercen las compañías prestadoras de servicios de internet a sus usuarios como los son *Facebook*, *Google*, *Yahoo*, entre otras, y mencionando el caso *Verizon*, la compañía de telefonía en Estados Unidos.

Aunque se mencionen las actividades realizadas en Estados Unidos, en la descripción del programa, se logra apreciar que el fenómeno alcanza dimensiones internacionales, ya que las compañías cuentan con la información de usuarios de todo el mundo. Si bien la vigilancia ejercida con drones y otros dispositivos es nombrada, no es el objeto de esta investigación.

Problema de investigación

La pregunta esencial de esta investigación es la siguiente: ¿Cómo influye el control de la vigilancia internacional en manos de corporaciones privadas en función de las revelaciones de Edward Snowden en relación al programa PRISM, al atributo soberano de vigilancia del Estado clásico? Para esto, es necesario contestar otras preguntas: ¿Cuáles

1 La organización Wikileaks fue creada en 2010 con el objetivo de publicar los secretos de Estado, de EEUU, esto incluye las actividades secretas que se llevan a cabo por dicho gobierno en el mundo, como el espionaje y actividades militares (Anónimo, 2015).

son las revelaciones relevantes sobre el programa *PRISM*? ¿Cuáles corporaciones privadas tienen el control sobre la vigilancia? ¿Cuál es el rol clásico del Estado con respecto a la vigilancia?, y en particular para el caso de Estados Unidos ¿Cómo accede el Estado a la información resultante de la vigilancia realizada por el programa *PRISM*?

Objetivos

El objetivo general de esta investigación es analizar la influencia en el ejercicio de los atributos soberanos del Estado de la capacidad de vigilancia internacional de las corporaciones privadas, conocida mundialmente a partir de las revelaciones de Edward Snowden sobre el programa *PRISM*.

Los objetivos específicos son:

Definir el ejercicio de los atributos clásicos soberanos del Estado sobre la vigilancia.

Describir las revelaciones más relevantes sobre el programa *PRISM*.

Enumerar y mencionar la capacidad de vigilancia de las corporaciones privadas implicadas en el programa.

Conocer el medio de acceso del Estado a la información resultante de la vigilancia realizada por el programa *PRISM*.

Estructura

Esta investigación se presenta en cuatro capítulos. En primer lugar, se encuentra el marco teórico, donde también se incluye el estado de situación relevado sobre el desarrollo y avances sobre el tema de esta investigación y los antecedentes del problema principal de la misma.

A su vez en el segundo capítulo, se analiza el concepto clásico del Estado y la vigilancia como atributo soberano de los Estados. La soberanía resulta un atributo esencial de los Estados independientes, que además en el modelo clásico son los únicos actores de las relaciones internacionales, sin embargo este concepto está ligado a los elementos del Estado que son el territorio, la población y el poder etático. El desarrollo de la tecnología e internet presentan un cambio en ésta realidad, donde las interacciones se realizan más allá de las fronteras, y los conceptos como seguridad, vigilancia y soberanía se encuentran mutando por estos nuevos fenómenos.

En el tercer capítulo, se describen los programas principales dentro de las revelaciones de Edward Snowden, poniendo especial atención en *PRISM*, que introduce cambios novedades en relación a otros programas de seguridad de la NSA, como por ejemplo el acceso directo de los proveedores para obtener la información de las personas del mundo.

Finalmente, en el capítulo cuatro, se describe como EEUU obtiene la información descripta en el programa *PRISM*, que involucra a corporaciones, como a otros Estados mediante alianzas.

En último lugar se presentan las conclusiones para dar un cierre y exponer los hallazgos de la investigación.

Hipótesis

La hipótesis que se infiere de la pregunta problema es: *El ejercicio de los atributos soberanos del Estado se ve influenciado por el control de la vigilancia internacional en manos de corporaciones privadas*.

CAPÍTULO I

Marco teórico

Considerando las diferentes teorías de las relaciones internaciones y los conceptos de seguridad altamente discutidos, el marco teórico de esta investigación se asienta en la teoría neorrealista, tomando como referente de la misma a Kenneth Waltz y en el concepto de la securitización aportado por la Escuela de Copenhague.

El neorrealismo (Salomón, 2002) toma como actor indiscutible de las relaciones internacionales al Estado, y ese es el enfoque de esta investigación. Más allá de que aquí también son de gran relevancia otros actores como lo son las corporaciones privadas, el que se destaca es el Estado. Tomando esta teoría, también se establece que los Estados son actores racionales y que se mueven según sus intereses. En este caso el interés a analizar es la seguridad la que pretende resguardar a través de la vigilancia. En el sistema anárquico de las relaciones internaciones, hay Estados que buscan tener influencia y conservarla frente a los demás. Aunque existan organismos internacionales que estipulen reglas, se toma de la teoría neorrealista que seguimos en anarquía internacional, ya que estos organismos no logran sobreponerse a los Estados. Sin embargo se toma el neorrealismo de Waltz y no el realismo, ya que también hay que tener en cuenta que si existen las instituciones internacionales y son actores internacionales relevantes, aunque no contrarresten la anarquía del sistema.

Uno de los principales intereses del Estado, en esta teoría y en el aporte de la escuela de Copenhague es la seguridad (Orozco, 2006). No obstante, ha habido demasiada discusión en torno al significado del término y hasta donde se expande.

La mayor concordancia con respecto al término, es que la seguridad se relaciona con la capacidad del Estado de defenderse de amenazas, tanto externas como internas. Y a su vez, en un primer momento esa capacidad parece estar íntimamente vinculada con el aspecto militar.

A pesar de esto, en los últimos años, se ha ampliado el concepto de seguridad, de modo que se incluye hasta la seguridad de cada uno de los habitantes del Estado, no solo contra amenazas contra su vida, sino también contra sus derechos, bienestar, entre otros.

La escuela de Copenhague (Orozco, 2006) introduce algunos elementos interesantes para la investigación, más allá de la discusión sobre el significado de seguridad. Establece que

la seguridad puede ser usada como un instrumento político, es decir que genere reacciones en las masas sobre toma de decisiones. A este hecho le van a adjudicar el término de *securitizar* –convocar voluntades para movilizar recursos-. A su vez, el objeto de referencia en esta investigación es el Estado como se ha mencionado, tomando de la Escuela de Copenhague a la teoría neorrealista para su abordaje. La propia Escuela plantea que la seguridad individual ha quedado desplazada muchas veces por la del Estado, por lo que podemos ver que la seguridad del Estado no es lo mismo que la seguridad de sus habitantes, por lo que se deja afuera en esta investigación las definiciones de seguridad que ponen énfasis en el bienestar de las personas y sus derechos.

Otro elemento importante que se añade a la definición de seguridad que afecta a esta investigación es el *speech act* que establece Waever (Verdes-Montenegro, 2015). Esto se relaciona con la seguritización y el mensaje que se da, cargado de cierto simbolismo que afecta las voluntades y puede incluir la movilización de recursos que caracteriza a la securitización.[2] Así la seguridad queda definida como un instrumento político para influir en voluntades y movilizar recursos, tomando como referencia a una amenaza al Estado.

Sin perjuicio de lo mencionado, el aspecto militar de la seguridad es de gran relevancia, pero en el siglo XXI vemos un cambio significativo en este aspecto, ya que los intereses del Estado en materia de seguridad no son solamente militares y ni tampoco exclusivamente armamentistas como sí lo era en la guerra fría, sino que el elemento del control de la información cobró otro papel.

En el gobierno de George W. Bush siguieron generándose grandes gastos militares. El período de Obama tuvo una política de acercamiento y "amistad", pero con gran contenido militar, gasto en guerras en Medio Oriente, y además se suman las develaciones de Edward Snowden sobre vigilancia a los usuarios de Facebook, Apple, y otras corporaciones privadas. También cabe mencionar las develaciones de Wikileaks sobre espionaje a otros líderes mundiales, como por ejemplo a la presidenta de Brasil en ese período, Dilma Rousseff (Anónimo, 2015). Aunque los últimos acontecimientos no estén incluidos en las definiciones de seguridad, aportan una nueva perspectiva a la definición, las ya emitidas por Waever (1993) y Buzan (1993), y lo expuesto por Moller (1996) son

2 Los términos securitización y seguritización serán utilizados indistintamente.

claves para explicar los últimos fenómenos relacionados a la seguridad, y en particular a la vigilancia internacional expuesta en esta investigación.

Asimismo, es pertinente definir el concepto de soberanía. El mismo, al igual que el concepto de seguridad se ha ido modificando con el tiempo y se ha discutido a lo largo del tiempo, ya que no tiene una definición única.

El concepto en sus inicios (Esnal, G., Ibarra, V., Jackson, M., Messano, F., Nieves, M., y Sabiguero, A., 2016) ha estado relacionado con la capacidad de imponer leyes y hacer que sean acatadas. Es una característica que poseen los Estados, por eso se habla de Estados soberanos. Arbuet da una definición parecida, agregando que hay un pacto entre los ordenados y los que mandan, que legitima dicha soberanía. El concepto está relacionado con el de Estado, y generalmente las personas que se rigen por determinadas leyes se encuentran en un determinado territorio (Arbuet-Vignali, Puceiro, 2010).

No obstante, uno de los puntos de cambio del concepto emerge con el surgimiento de internet, donde ya las actividades de las personas traspasan los límites territoriales.

Marco conceptual

El principal marco conceptual de esta investigación se complementa con los conceptos vertidos por el libro de Greenwald "*No place to hide*" (2014), que además de describir todos los puntos trascendentes sobre las develaciones de Edward Snowden sobre el programa PRISM, entre otros, relata como Edward Snowden se hizo de esa información, como contactó a los periodistas que divulgaron la información (entre ellos, el propio Greenwald) y el papel de la administración de Obama sobre la NSA y sobre PRISM.

También es importante definir otros conceptos como son el de soberanía, seguridad y vigilancia.

El concepto de soberanía ha sido ampliamente discutido y ha ido evolucionando (Esnal et al., 2016). El concepto clásicamente está asociado con la capacidad de imponer leyes. Arbuet (2010), sin embargo, establece que sí requiere el cumplimiento de reglas, pero que éstas son pactadas por los que mandan y los ordenados. Sin duda se trata de una fuerza legitimante para hacer acatar las normas (Arbuet-Vignali, Puceiro, 2010).

A su vez, la otra característica que tiene la soberanía es su territorialidad (Esnal et al., 2016), la visión neorrealista entiende a la integridad territorial del Estado como un

elemento sustancial para el alcance de la seguridad y la soberanía, no obstante esto se ha visto transformado con el advenimiento de internet, donde no existe la territorialidad y plantea un desafío para la clásica soberanía estatal. Las actividades llevadas a cabo en internet trascienden al Estado y a sus reglas. Esto plantea un nuevo escenario y los neorrealistas lo ven como un riesgo a la soberanía. Además internacionalmente, la soberanía se vincula con el sistema de coordinación, donde los Estados deciden sus-leyes. Internamente los Estados se ven amenazados por el surgimiento de internet, externamente también, pero en particular por nuevos actores internacionales que tiene capacidades iguales o incluso mayores al Estado, como lo son las corporaciones internaciones. Esto lleva a pensar que el Estado puede perder su protagonismo en la escena internacional.

La ciberseguridad es otro de los conceptos claves de esta investigación. La misma es una rama específica dentro de la seguridad que ha surgido a partir de ciertos fenómenos de la actualidad. La seguridad (Esnal et al., 2016) ha adquirido características multidimensionales con estos nuevos fenómenos como lo son internet y el desarrollo de la tecnología. Esta transformación lleva a que el concepto clásico de seguridad no cubra los aspectos relevantes que aparecen en la actualidad.

El Estado (Esnal et al., 2016) clásicamente se ocupaba de la seguridad interna y externa. La externa se basaba tradicionalmente en evitar las amenazas de otros Estados a su integridad, mientras que la interna busca repeler amenazas hacia su población e instituciones que se puedan generar dentro de los límites del propio Estado.

No obstante, este concepto clásico no aplica a las necesidades actuales, donde la amenaza puede surgir de sitios como internet, donde algunas de las principales amenazas son los hackers y ciberterroristas.

Los hackers son en su mayoría programadores que consideran que deben hacer de público conocimiento todo tipo de información, incluso la secreta o confidencial. La ética del hacker, lo obliga a facilitar el acceso y la información a la mayor parte de personas posible. A su vez, se dividen en dos tipos: los *white hat* y los *black hat.* Estos últimos son los que cometen ilícitos en internet, y son considerados una amenaza mayor, debido a sus objetivos, que tienen que ver más con una ganancia personal, a diferencia de los *White hat* que también cometen ilícitos pero con la convicción de que es algo de interés público, por ejemplo cuando roban información clasificada para compartir con personas que no pueden acceder a la misma, pero que es de su interés. Los hackers son amenazas para el

Estado, ya que pueden desde crear virus y dañar información, como también robarla (Pilnik, 2017).

Además estos nuevos actores pueden actuar traspasando las fronteras de los Estados, ya que actúan en internet (Pilnik, 2017), donde desaparecen los clásicos elementos del Estado, como lo son el territorio y el poder etático.

El ciberterrorismo es la forma de terrorismo que se realiza en internet. El terrorismo se puede definir como actos que buscan generan terror (Ibarra, Nieves, 2016). En este caso los que generan este terror son *black hats* organizados (Pilnik, 2017).

La ciberseguridad se basa en evitar amenazas hacia la información y activos críticos del Estado. Está vinculada con la seguridad nacional. Un ejemplo para entender la definición de la misma es precisamente el programa PRISM, donde el Estado y ciertas corporaciones actúan en conjunto para almacenar información con la excusa de protegerse de amenazas, principalmente del protagonista de lo que va del siglo XXI: el terrorismo.

El programa *PRISM* surge en la NSA[3]. Este tiene como fin la recolección de datos masivos de los usuarios de diversas redes sociales o incluso dispositivos de empresas norteamericanas, como lo son *Google*, *Facebook*, *Yahoo*, *Apple*, *Microsoft*, entre otras. Tiene la particularidad, precisamente, de que la información proviene directamente desde los *servers*, es decir, las corporaciones mencionadas. Nace en la administración de Bush pero continúa en la administración de Obama (Greenwald, 2014).

Cabe destacar que aunque esta investigación reúne a modo de antecedentes datos desde 2006 cuando nace Wikileaks, el programa PRISM surge en 2007, y los datos expuestos son de los últimos años del programa, desde 2011 a 2013, de donde surgen las principales revelaciones de Snowden (Greenwald, 2014).

Edward Snowden se hizo de la información, cuando se encontraba trabajando para la NSA en Hawaii, su posición le daba ciertos accesos, más allá de que tuvo que tomar ciertos recaudos a la hora de salir con dicha información de las instalaciones donde trabajaba (Poitras, 2014).

El programa *PRISM*, almacena la información de los usuarios a nivel mundial. La supuesta justificación de esto es la seguridad nacional y la lucha contra el terrorismo,

3 NSA significa *National Security Agency*, en español: Agencia de Seguridad Nacional.

aunque al fin de cuentas, parece relacionarse poco, pero esto es algo a ser desarrollado más adelante.

Lo importante a destacar en esta instancia sobre el programa es que los que tienen el acceso a esta información son las mencionadas compañías de dimensiones globales, pero que esta información llega a la NSA, a pesar de que existe el derecho a la privacidad, que es aplicable a lo que las personas publican o buscan en internet.

Cuando esto sale a la luz, lo que se logra una vez que Edward Snowden contacta a Glenn Greewald y a Laura Poitras mediante mails y chats encriptados[4] solicitándoles que viajen a Hong Kong a reunirse con él, las empresas dijeron no tener ningún relacionamiento con el programa *PRISM* (Poitras, 2014).

Lo que se menciona como la administración de Obama, refiere al periodo de presidencia de 2009 al 2017, y también es otra categoría importante, ya que este es el presidente de los Estados Unidos, durante todo el período que será analizado en esta investigación el programa *PRISM*.

Además subyacen relaciones entre las empresas y los Estados para la recolección de información (Ramonet, 2016), además de que el espionaje y diplomacia secreta, juegan un rol principal. Ignacio Ramonet se refiere a una alianza entre las empresas y los Estados. Sin embargo esta bibliografía no solo recopila información como la de Glenn Greenwald, sino que además tiene muy incorporado el punto de vista del autor, que esta investigación no busca cuestionar, pero que es de utilidad principalmente los datos primarios de los autores para poder sumar elementos de análisis a la investigación.

"*Citizen four*" de Laura Poitras y "*We steal secrets: the story of wikileaks*" de Alex Gibney aportan otros elementos. El documental de Laura Poitras contiene las mismas categorías de análisis que Glenn Greenwald, pero esta vez desde el material audiovisual. Sin embargo, el material de Alex Gibney es utilizado para poner ejemplos sobre Wikileaks. La categoría de análisis que trae el trabajo de Alex Gibney como el libro "*The wikileaks files*" de autor anónimo, es precisamente Wikileaks y nos introduce nombres como Julian Assange y Chelsea Manning, que escapan al tema principal de la

4 Encriptar en una trasformación predeterminada que se le aplica a un dato que hace que no se pueda entender por terceros, ya que hay que tener una clave en común para descifrarlo (Greenwald, 2014).

investigación pero son mencionados y además contribuyen a marcar el comienzo del tiempo acotado en el objeto de estudio.

Wikileaks es una organización que se caracteriza por buscar fuentes de información secreta sobre los gobiernos del mundo, también contribuye a que sus usuarios accedan a chat encriptado y aprendan a "escaparse" del control que hay en internet. Su fundador principal es Julian Assange, pero la fuente de una de las principales develaciones de la que se hizo la organización, es Chelsea Manning, un ex militar del gobierno de los EEUU.

Algunos desarrollos sobre el tema:

A pesar de que la temática es de relativa novedad, ha habido varias investigaciones con respecto al tema de la ciberseguridad, la vigilancia internacional y los cambios en los atributos soberanos clásicos del Estado. Dichas investigaciones sirven como antecedentes de la presente, e introducen conceptos y preguntas que enriquecen el análisis del tema.

En el libro de Ignacio Ramonet "Imperio de la vigilancia" (Ramonet, 2016) se menciona una alianza entre Estados y empresas. Establece que el tema de la seguridad ya no es exclusivo del Estado, sino que se ha privatizado en manos de las grandes compañías de informática y telecomunicaciones. Esto también genera que la vigilancia llegue a lugares anteriormente inimaginables, ahora es a todo el mundo y todo el tiempo.

Para este autor, actualmente el "Imperio de vigilancia" tiene varios componentes como son el Estado, su aparato militar y las grandes industrias de internet. Es importante saberlo todo, no solo algunos aspectos de las vidas de las personas. Esto deriva en la desaparición de la vida privada.

A su vez en su libro se nombran algunas alianzas entre Estados para recabar mayor información. El UKUSA o *five eyes*, es una alianza entre los servicios de información de EEUU, Inglaterra, Australia, Canadá y Nueva Zelanda. Fue iniciada en 1946 para prevenir riesgos en la seguridad de cada uno de los Estados mencionados.

Ignacio Ramonet concluye que controlando la información se controla el comportamiento, no solo de los individuos, sino también de instituciones.

El artículo "Relaciones entre soberanía y tecnología en tiempo de internet" (Esnal et al., 2016) detalla principalmente la evolución del concepto de soberanía, explicando cómo se ha dado dicha evolución y cómo afecta el fenómeno de internet al concepto, así como a

otros atributos del Estado. Plantea que hay una crisis del Estado, con respecto a cómo era concebido tradicionalmente, en un momento donde hay un nuevo espacio social, los actores transnacionales tienen la misma relevancia internacionalmente que los Estados (los que solían ser los actores principales del sistema), y donde hay una desterritorializacion de las actividades económicas. Este antecedente es de gran relevancia a esta investigación, introduciendo conceptos claves y planteando cuestiones similares con respecto al papel actual de Estado con respectos a los nuevos fenómenos del siglo XXI.

En el artículo "La seguridad internacional determinada por un mundo online: el Estado ante el desafío del terrorismo y la ciberseguridad" (Ibarra, Nieves, 2016) también se presentan conceptos que son claves para este trabajo y es un claro antecedente de este. En el mismo se plantean los cambios en el concepto de seguridad, también ligados a los nuevos fenómenos del siglo XXI. Sin embargo aquí se pone énfasis en el caso de las nuevas amenazas y riesgos del nuevo escenario internacional, como lo es principalmente el terrorismo. Tanto esta amenaza, como el narcotráfico y el crimen organizado se han transnacionalizado. El terrorismo pasa a ser un actor más del sistema internacional generando consecuencias no solo físicas, como también impacto psicológico. Estos fenómenos no se desarrollan solo de manera física, sino que también en internet, generando conceptos como la ciberseguridad y el ciberterrorismo. Pese a que el terrorismo no es de vital importancia para este trabajo, la ciberseguridad es un concepto de real relevancia a la hora de explicar los acontecimientos que se están generando en internet y como defenderse de las amenazas, sean por parte de los Estados, las corporaciones, o los ciberterroristas.

El aporte más trascendente del artículo "La distopía ya está aquí: Vigilancia estatal, de Orwell a Snowden y El Guardian" (Osaba, 2015) intenta asociar el caso internacional de la vigilancia con el nacional. Uno de los aportes más grandes de este artículo es su carácter filosófico acerca de esta vigilancia total, la cual también era mencionada por Ignacio Ramonet, comparándola con la novela de George Orwell, 1984, donde la vigilancia es constante y no es un mero ojo observador, sino que además controla a los ciudadanos inclusive en sus pensamientos.

En el caso del libro "*No place to hide*" (Greenwald, 2014) se compila lo más destacable de las develaciones de Edward Snowden. Glenn Greenwald, es uno de los periodistas que le hace la entrevista a Edward Snowden una vez que el se hace de información

confidencial de las oficinas de la NSA en Hawaii, y emprende viaje a Hong Kong donde se comunica con Laura Poitras y con Glenn Greenwald para llevar a cabo la publicación de esta información al mundo entero. En "No place to hide" se narra toda esta situación adjuntando emails que lo avalan, así como contenido de las presentaciones que se muestran en la NSA en cuanto al programa *PRISM*, y otros programas que son mencionados. Esta reunión de material es un antecedente que aporta toda la información que hay disponible sobre las develaciones de Edward Snowden. No obstante, se realiza una compilación muy parecida en el material audiovisual de Laura Poitras "Citizenfour" (Poitras, 2014).

Además, la OEA realizó una investigación sobre seguridad cibernética en América Latina y el Caribe (2014). En las "Tendencias de Seguridad Cibernética en América Latina y el Caribe" se destacan la cooperación regional frecuente y con un papel relevante para combatir los peligros cibernéticos y el avance con respecto a políticas, leyes y capacidad técnica para enfrentar el nuevo fenómeno. Sin embargo, la investigación de la OEA sugiere poner aún más esfuerzo en estas áreas y que los países que no han avanzado copien las actividades de los países que sí lo han hecho. A su vez, explica que internet ha favorecido al aumento de delitos como lo son la pornografía infantil, la trata de personas, el tráfico de armas, entre otros; y ha generado nuevos delitos como el robo de identidad para cometer fraude, secuestro de información por dinero, y otros tipos de hackeo.

El informe, también, menciona algo que toca directamente a esta investigación y es que se plantea la filtración de información gubernamental, y pone de ejemplo el caso de EEUU. Aunque no mencione concretamente a las develaciones de Edward Snowden, las de Chelsea Manning, y las publicaciones de Julian Assange, sin duda estas han sido los momentos clave donde la información confidencial gubernamental se vio violada, y todos estos son sucesos anteriores al informe. El mismo, invita a que los gobiernos y las corporaciones privadas unan información y combatan juntos el delito informático.

Franco Pilnik, en su libro "Delitos en el ciberespacio" describe la historia de internet, define el ciberespacio como un nuevo lugar, donde no hay fronteras, ni los elementos clásicos del Estado, sino que el espacio es virtual y todo se desarrolla en internet. Está más allá de la soberanía del Estado (Pilnik, 2017).

Antecedentes

El surgimiento de una dimensión del terrorismo generó un cambio en las reglas de juego dentro de EEUU, como a nivel mundial (Ramonet, 2014), y en el siglo XXI ya es otro actor del sistema internacional (Ibarra, Nieves, 2016).

El terrorismo en sí, no es un fenómeno nuevo pese a que su significado actual sí es nuevo. Se entiende como terrorismo a la dominación por el terror y el concepto se genera en la revolución francesa cuando Maximilien Robespierre instaura "el terror" para hacerse del poder político (Ibarra, Nieves, 2016). Más adelante se lo asocia con un acto contra el Estado, que además causa terror, y no se consideran solo los actos físicos, sino los que afectan psicológicamente a un determinado grupo de personas.

En la última década del siglo XX, con la caída de la URSS y la preponderancia de EEUU (Ramonet, 2014), se generó un auge del neoliberalismo y la democracia. No obstante, la escena internacional cambió luego de los atentados del 11 de septiembre de 2001 a las torres gemelas, en EEUU. Se empezaron a aplicar medidas de seguridad más rigurosas, por ejemplo en los aeropuertos.

Esto sirvió como principal excusa para llevar a cabo el control total que engloba el programa PRISM descripto por Edward Snowden (Ramonet, 2014). Las autoridades de EEUU, incluso el mismo Obama se refirió al terrorismo para justificar las actividades realizadas por la NSA.

Según las autoridades de EEUU (Poitras, 2014) se realizaron dichas actividades para poder garantizar la seguridad nacional, es decir evitar cualquier tipo de acto terrorista que pueda surgir.

Luego de los atentados del 11 de septiembre, un joven Edward Snowden, compartía pensamientos en una especie de *blog* con un usuario llamado *The TrueHOOHA*. En este momento a Edward Snowden le sucedía lo que a muchas personas en el mundo: quería acabar con el terrorismo y sentía la obligación de ayudar a liberar a las personas de la opresión que se vivía en Iraq (Harding, 2014). Esto lo llevó a querer ser militar, pese a que su corta visión y un accidente hicieron que llevara otro camino que lo acercaría lentamente a la NSA y luego a las posteriores revelaciones.

Además de los atentados del 11 de septiembre, las publicaciones realizadas por la organización Wikileaks también tuvieron efecto en las revelaciones de Edward Snowden (Poitras, 2014).

Wikileaks había estado publicando información confidencial, principalmente sobre espionaje de EEUU a otros países del mundo (Anónimo, 2015). Sin embargo esta información había sido colgada en la web como material bruto y sin ninguna contextualización. Además gran parte de lo publicado tenía fuentes anónimas, pese a que es conocido el nombre de quien funda la página, que es Julian Assange. El anonimato como bien explica Edward Snowden (Poitras, 2014) genera persecución que puede generar problemas a inocentes. Así mismo se tiene el caso de Chelsea Manning, que sí brindó información a Wikileaks, pero fue traicionada y tuvo que ir a prisión, de donde salió gracias a la presión social y demostrar arrepentimiento (Gibney, 2013).

Estos hechos generaron que Edward Snowden no sólo revelara la información con pruebas de los programas y actividades de la NSA, así como también llevó a que contactara a un periodista para publicar los datos, dándole credibilidad a la información expuesta, y a que decidió entregar este material develando su identidad y rostro, para que no hubiera una persecución a otros empleados de terciarizadas que tuvieran acceso a dicha información. A su vez justificó esta decisión en balancear el nivel de los ciudadanos y el Estado. El anonimato generalmente se encuentra asociado al miedo y los ciudadanos no deberían tener miedo de su propio Estado que es la entidad que los debería proteger (Poitras, 2014).

Asimismo en el gobierno de George W. Bush se crea una ley antiterrorista, llamada ley *Patriot Act.* Esta permite arrestar a sospechosos de terrorismo, ser privados de libertad y hasta poder allanarle su hogar sin ningún tipo de autorización judicial y espiar sus comunicaciones tanto telefónicas como por correo electrónico. Esto dio gran poder al gobierno de Estados Unidos, ya que incluso aprisionaba a personas sin ningún tipo de juicio. También al ser liberados, muchas veces se los envía a países de donde no son nacionales y no tienen ningún tipo de relacionamiento. Como ha sucedido con los presos de la base de Guantánamo (Ramonet, 2016).

También en el gobierno de George W. Bush se crea un programa secreto. Este es un claro antecedente de *PRISM* y de los demás programas de vigilancia masiva, donde en 2008, se llevó a cabo un programa secreto en los que se intervenían las comunicaciones

telefónicas de civiles, que probablemente nada tenían que ver con Al Qaeda, sin embargo se realizan con la excusa de detener el terrorismo luego de los acontecimientos terroristas sobre el World Trade Center el 11 de Septiembre del 2001 (Greenwald, 2014).

Jack Balkin, profesor de derecho en Yale, confirmó que la corte de la FISA (tribunal de vigilancia de inteligencia extranjera de Estados Unidos) autorizó este programa promovido por George W. Bush.

Como el gobierno de EEUU se organizaba en materia de seguridad materializando estos actos en programas y leyes, los *hackers* también hacían su parte. La ética *hacker* (incluso la de los *White hat*) supone un deber de revelar todo lo que se considere de interés público, así como facilitar el acceso a internet y a toda la información (Pilnik, 2017). Aaron Swartz es un claro caso de lo que un *hacker* siente que debe hacer. En 2008, Aaron Swartz bajó datos de PACER [5] (datos electrónicos de la Corte Federal de EEUU) la cuál era pública pero había que pagar por cada página descargada. Como los datos que había descargado Aaron Swartz eran menos del 20% del total, no tuvo consecuencias. No obstante, luego volvió a descargar datos pero está vez, el 100% de las publicaciones académicas de JSTOR, por esto si fue acusado pero no cumplió la pena porque se suicidó antes de compadecer al juicio.

5 Public Access to Court Electronic Records (PACER).

CAPÍTULO II

Concepto clásico de soberanía del Estado y situación actual con respecto a la vigilancia en manos de las corporaciones**.**

La soberanía es un atributo esencial de los Estados independientes (Arbuet-Vignali, Puceiro, 2010), que hace a los mismos, ya que en lo interno resulta en una fuerza legitimante sobre la cual recae el poder de una autoridad suprema que regula el funcionamiento, como a su vez externamente nadie puede inferir en los asuntos internos, y además participa en la creación de las normas a las que se somete en sus relaciones con otros Estados. Sin embargo, el concepto de soberanía e incluso sus elementos esenciales se han cuestionado en los últimos tiempos debido a nuevos fenómenos que han cambiado las reglas de juego en las relaciones internacionales (Esnal et al., 2016).

Concepto clásico de Soberanía

Para que una comunidad política pueda existir como tal, es necesario que una autoridad superior la regule, independientemente de que sea legítima o no (Arbuet-Vignali, Puceiro, 2010). No obstante, en el marco del derecho internacional público es necesario que se cumplan ciertos requisitos para que sea legítimo. Pese a que los requisitos no son de relevancia para esta investigación, sí lo son sus efectos.

Que un Estado sea soberano, tiene efectos internos como externos (Arbuet-Vignali, Puceiro, 2010). El atributo de la soberanía clásicamente se entiende como exclusivo de los Estados independientes, que a su vez, eran los actores principales de las relaciones internaciones. Incluso la existencia de los demás actores estaba en cierta discusión. En el ámbito interno le daba fuerza legitimante como para tomar decisiones y usar la fuerza en caso de que no se cumplieran las reglas. Generalmente la organización política y las reglas son pactadas con los que acataran las mismas. En el plano externo también genera efectos, como la independencia e igualdad ante todos los demás Estados y la participación del sistema de coordinación en donde está inmerso en el ámbito internacional, es decir que no se le pueden imponer normas, sino que participa de la creación de las mismas y que además las acepta mediante tratados u otros instrumentos.

El poder único y supremo que tiene el Estado genera efectos dentro de un cierto territorio.

Los elementos esenciales de los Estados clásicamente son territorio, población y poder etático. Es decir que hay un cuerpo de reglas que regulan a la población, que además se

encuentran dentro de sus fronteras. El territorio a su vez incluye el suelo, espacio aéreo, y aguas, teniendo así en cuenta el espacio tridimensional.

Nuevos fenómenos

Los nuevos fenómenos que han surgido después de la guerra fría y principalmente en los primeros años del siglo XXI, han marcado un quiebre con respecto a las concepciones clásicas que se tenían del Estado, la soberanía y la seguridad.

Los fenómenos más relevantes son el desarrollo de la tecnología e internet (Esnal et al, 2016). Ambos han generado lo que se conoce como la sociedad de la información, donde ya los Estados no tienen un lugar central como siempre han tenido en la escena internacional.

Primero los elementos esenciales del Estado- Nación, ya no son alcanzados por los nuevos fenómenos desde la perspectiva clásica. Digamos que cada uno de sus elementos ya no puede ser ordenado por los Estados. El ejemplo más claro y visible, es el del territorio.

Un fenómeno de las características de internet trasciende las fronteras. Las interacciones que se llevan a cabo en línea son diversas y parten de distintos lugares del mundo, incluso hay algunas de las que no se puede saber su procedencia en específico. En Internet si se intercambia y maneja información, y la misma no es algo que se pueda establecer en un lugar físico. Hay intentos por parte de varias organizaciones intergubernamentales como la OEA (Ibarra, Nieves, 2016) que buscan la forma de regular esa información, tomando en cuenta donde se generó, o el lugar donde están las computadores o servidores que almacenan la información, pero la situación aún no es muy clara al respecto. Claramente todas estas actividades que se llevan a cabo en Internet van más allá de lo que los Estados pueden manejar y ordenar.

Otro condicionamiento tiene que ver con la propia infraestructura para el acceso a la información (Ibarra, Nieves, 2016). Es esencial tener ciertos recursos para poder acceder a la información. Ya los Estados no están tan adelantados en estos ámbitos, es decir que no tienen el dominio y desarrollo de ciertas tecnologías, como sí lo tienen los actores privados, como las corporaciones globales. Esto genera un nuevo desafío para el Estado, ya que es el sector privado el que posee la información y la infraestructura para acceder a la misma, como el permiso de sus usuarios.

Las actividades que se llevan a cabo en internet son tanto económicas, como sociales y culturales, por lo que abarca un espectro muy amplio, que no es capaz de ser cubierto por los Estados.

El neorrealismo establece esto mismo (Esnal et al., 2016), la base territorial era esencial para la soberanía, y para que el Estado pueda cuidar de su propia seguridad. Internet por esto mismo, pone en riesgo a la soberanía y al Estado como lo hemos conocido durante los últimos siglos. El Estado ya no puede controlar totalmente lo que sucede en su territorio.

Además del problema del territorio, aún es complejo pensar en un marco jurídico que regule las interacciones que se dan en Internet. Se puede entender también que regularlo viola el derecho de libertad de acceso y de expresión que hoy en día se puede lograr en la web. Sin embargo, los usuarios quedan atados a normas impuestas por las corporaciones, y el Estado no logra proteger a sus ciudadanos de esas condiciones. Esto también hace tambalear al concepto de seguridad con el de soberanía.

En realidad la seguridad es, según Thomas Hobbes, una de las causas del nacimiento del Estado-Nación (Ibarra, Nieves, 2016) ya que el Estado brinda cuidado físico a su población, por lo que es parte de la esencia del Estado. No obstante, internet, el uso comercial de internet y el acceso que es posible en la actualidad cambia completamente estos conceptos teóricos sobre el Estado.

Así como el neorrealismo entiende que la soberanía se pone en riesgo en estos términos, también hay autores que entienden que la soberanía ha cambiado y ya no se la puede definir como ha sido definida (Esnal et al., 2016). Lo mismo sucede con el concepto de seguridad que ha sido transformado y se entiende en primer lugar que se debe ver como multidimensional (Ibarra, Nieves, 2016). Además de que la seguridad se haya ampliado a varios ámbitos, en el caso de internet se ha generado un nuevo concepto de la misma, que es el de ciberseguridad, este tiene que ver con la seguridad de la información digital pero relacionada con la seguridad nacional, es decir salvaguardando dicha información se protege al Estado y a sus ciudadanos. A pesar de que esto pueda parecer algo beneficioso, es imposible en el mundo actual para los Estados no participar con el sector privado en materia de ciberseguridad, y uno de los efectos contrarios que se destacan es la perdida de la privacidad.

Nuevos actores de gran importancia: corporaciones transnacionales

A pesar de que clásicamente, el actor indiscutido de las relaciones internacionales era el Estado, en el siglo XXI las corporaciones transnacionales tienen un peso igual o mayor que el Estado. Esto se debe no solo al poder económico que poseen, sino que además son dueños de gran parte de la información que circula en internet (Esnal et al., 2016).

Las corporaciones tienen la infraestructura para almacenar cualquier cantidad de datos, y cuando ofrecen servicios a los usuarios, a cambio obtienen la información que los mismos brindan de forma voluntaria, o incluso involuntaria cuando aceptan términos que no leen o ni cuestionan para formar parte de las interacciones que se llevan a cabo en Internet, como lo son las redes sociales. También brindan información de manera involuntaria cuando compran dispositivos tecnológicos que funcionan como instrumentos de escucha o incluso como transmisor de imágenes como puede ser un celular o una computadora (Greenwald, 2014).

Toda esta situación pone a las corporaciones en una posición superior a los Estados en materia de seguridad. El sistema internacional se vuelve más complejo y estos nuevos actores ponen en riesgo la soberanía del Estado, como también lo desplazan de su lugar protagónico de las relaciones internacionales (Esnal et al., 2016). La vigilancia que era uno de los atributos esenciales de la soberanía y tema exclusivo de los Estados, se ha privatizado (Ramonet, 2016). La OEA incluso incluye al sector privado para poder reforzar la ciberseguridad (Ibarra, Nieves, 2016), esto es una novedad de este siglo, ya que este tipo de organizaciones operaba entorno a los Estados, pero ahora es indispensable la participación de dichas corporaciones ya que son las que tienen la infraestructura y la información como para llevar a cabo cualquier tipo de operativo de seguridad cibernética.

Sin embargo, todo esto genera mucha incertidumbre (Ibarra, Nieves, 2016) sobre el futuro de las relaciones internacionales y el lugar que tendrán los Estados y las corporaciones, aunque parece que las últimas van ganando poder en el escenario internacional.

Cabe destacar que el tema de la seguridad ha cambiado significativamente luego del atentado a las torres gemelas el 11 de septiembre (Ibarra, Nieves, 2016). Esto marcó un quiebre en materia de seguridad, y llevó al desarrollo que tenemos hoy en día, donde hay una vigilancia total (Ramonet, 2016).

Este hecho, más los avances tecnológicos, generan los acercamientos entre los Estados y las corporaciones, que al menos en principio cooperaron para obtener información de personas para anticipar atentados terroristas o llegar a los responsables. Pese a esta justificación, el tema es muy discutido, ya que se está vulnerando el derecho a privacidad, en un lugar donde parece raro si un usuario no quiere revelar sus datos porque podría pensarse que oculta algo (Ramonet, 2016).

Más allá de la incertidumbre que se ha generado en el ámbito internacional, lo que es claro es que el lugar de los Estados ha cambiado y ya no es el actor único y principal de las relaciones internacionales. La información pertenece a las corporaciones globales y esto les da poder (Ibarra, Nieves, 2016), ya que atributos esenciales de la soberanía que siempre fueron ejecutados por los Estados, hoy están en manos de corporaciones, como lo es la seguridad.

CAPÍTULO III

Las revelaciones de Edward Snowden

Edward Snowden, momentos previos a las revelaciones, trabajaba para Booz Allen Hamilton, una empresa subcontratada por la NSA (Agencia de seguridad Nacional de Estados Unidos), y es de donde extrae la información que decide compartir al mundo entero (Greenwald, 2014).

Debido a la relevancia de la información y las diversas interpretaciones que se pueden generar de recibir el material sin editar por parte del público, Edward Snowden decide contactar a la cineasta Laura Poitras y al periodista y abogado Glenn Greenwald, para publicar dicha información (Greenwald, 2014).

Los contacta mediante mensajes encriptados que son bastante confusos y despiertan ciertas sospechas en Glenn Greenwald, más aún, cuando Edward Snowden los convoca para la revelación de la información en Hong Kong, ya que podría tratarse de un fraude. Sin embargo decidieron ir a comprobarlo y efectivamente Edward Snowden poseía información confidencial sobre los programas de vigilancia masiva que estaba llevando a cabo la NSA.

Glenn Greenwald una de las primeras preguntas que le plantea a Edward Snowden es la motivación de la exposición del material, así como de su identidad, ya que estaba poniendo en riesgo su libertad o incluso su vida. Él revela que debe hacerlo de esa forma para balancear el poder entre los ciudadanos y el gobierno, el miedo de los ciudadanos hace que ese poder no este balanceado, sino que todo lo contrario, que se pueda manipular y vigilar a los ciudadanos de cualquier manera. (Poitras, 2014)

De esta forma comienzan las revelaciones a ser transmitidas al principio por *The Guardian* y luego por otros medios de prensa. (Poitras, 2014).

Misión de la NSA y el objetivo de los programas.

La misión de la NSA, es clara y aparece en todos sus programas llamada *collect it all*, es decir, recolectarlo todo. (Greenwald, 2014). Recolectarlo todo implica, que la NSA sea capaz de tener información sobre todas las comunicaciones, localizaciones, actividades, movimientos, preferencias de todos los ciudadanos del mundo entero. (Greenwald, 2014).

Este tipo de información se clasifica de dos formas. Existe la información de contenido y los metadatos. Los primeros refieren por ejemplo, al contenido de los emails que alguien pudo enviar, lo que habla por teléfono, lo que busca en internet, entre otros. Y los metadatos tienen que ver con la información de ese contenido, por ejemplo, números de teléfonos a los que se llaman, o de las llamadas recibidas, localización de las personas, etc. (Greenwald, 2014).

Cuando salieron a la luz las relevaciones de Edward Snowden (Greenwald, 2014), la NSA manifestó tener información sobre los metadatos pero no la información de contenido. Esto es refutable con las pruebas brindadas por Edward Snowden. Más allá de esto, los metadatos pueden dar información crucial sobre las personas y claramente invade igualmente la privacidad.

Principales programas

BOUNDLESS INFORMANT

Una de las primeras relevaciones fue el programa *boundless informant* (Greenwald, 2014), en español podría ser traducido como informante sin límites. En dicho programa el objetivo es recolectar las llamadas e emails de todo el mundo.

Este fue uno de los primeros escándalos, ya que el jefe de la NSA, Keith Alexander, negó que se llevaran a cabo este tipo de programas, ante el congreso de EEUU. La operación tenía un acceso global, y había recolectado más de tres mil millones de emails y llamadas.

Lo que también generó escándalo (Poitras, 2014) es que la operación tuviera como objetivo a cualquier civil, sin que existiera algún tipo de sospecha de estar relacionado con alguna agrupación terrorista, sino que el objetivo eran todas las personas del mundo. Para este tipo de programas se contó con alianzas con compañías telefónicas y tecnológicas como *Verizon*, *Microsoft*, *Motorola*, *AT&T*, *CISCO*, *Oracle*, *EDS*, *Qualcomm*, *Qwest* y *H-P*.

FAIRVIEW

Similar a *boundless informant* (Greenwald, 2014), *Fairview* es un programa que tiene como objetivo la recolección de información sobre llamadas telefónicas. Ésta vez con acceso a cables internacionales, routers y switches. El objetivo del programa nuevamente es global.

OAKSTAR

Asimismo este programa busca detectar comunicaciones, pero esta vez el objetivo está en el extranjero, buscando socios en el exterior. Esto permitió interceptar comunicaciones en Brasil y Colombia (Greenwald, 2014).

STORMBREW

Este programa se llevó a cabo junto con el FBI, y su objetivo es determinar ciertos puntos precisos a vigilar, a los que se les dio nombres clave (Greenwald, 2014). Además de los proveedores norteamericanos de telecomunicaciones de los que se disponía (*ARTIFICE* y *WOLFPOINT*), se manejaron cables submarinos para el acceso, uno en la costa oeste y el otro en la costa este de EEUU.

PRISM

El programa *PRISM* aporta varias novedades con respecto a los anteriores (Greenwald, 2014). El objetivo vuelve a ser global pero está vez es mucho más plausible, ya que la NSA en este caso se provee directamente de los servidores más grandes a nivel mundial, como lo son las compañías *Microsoft*, *Yahoo*, *Google*, *Facebook*, *Paltalk*, *AOL*, *YouTube*, *Skype* y *Apple*.

En este programa la vigilancia es total (Ramonet, 2016), todo puede ser espiado y archivado, y también transmitido a las otras agencias de EEUU, como lo son el FBI y la CIA. El alcance es completamente masivo.

No sólo tiene que ver con la información disponible en línea, sino que también los dispositivos electrónicos como celulares y computadores, funcionan como dispositivos de escucha y video cuando la NSA lo desee (Poitras 2014). Según el propio Edward Snowden es el momento que en la NSA ha recolectado más información en la historia (Poitras, 2014) y prácticamente nadie en el mundo puede escapar de esta vigilancia masiva. Ya que a todo lo mencionado se suman drones que también vigilan a los ciudadanos, o incluso las cámaras de las ciudades. Nuestros teléfonos inteligentes además de ser dispositivos de escucha y video, son un GPS constante de las actividades que realizamos en el día. Así como también lo son nuestras tarjetas de crédito.

Ignacio Ramonet (2016) lo compara con la novela 1984, de George Orwell, ya que también hasta los televisores inteligentes nos pueden vigilar, algo que podría parecer de ciencia ficción, el programa *PRISM* lo hizo una realidad.

A su vez, *PRISM* no solo involucra a las grandes compañías mundiales, sino que además llevó a Estados Unidos a generar alianzas para compartir información con otras potencias y que el alcance sea aún mayor. Todo está intervenido y es clasificado (Poitras, 2014).

Corporaciones implicadas en PRISM

Las corporaciones implicadas en el programa *PRISM* según las revelaciones de Edward Snowden, son *Microsoft*, *Google*, *Yahoo*, *Facebook*, *Paltalk*, *Youtube*, *Skype*, *AOL* y *Apple* (Greenwald, 2014)

Todas estas grandes compañías son estadounidenses, pero brindan sus servicios en todo el mundo. Prácticamente cualquier ciudadano del mundo utiliza alguna de ellas, con fines recreativos, para comunicarse o incluso para buscar información. De este modo, tienen un carácter avasallante en la vida de las personas del siglo XXI que tienen acceso a internet.

GAFAM y objetivos de las corporaciones

Las corporaciones llamadas *GAFAM*, son una red de gigantes corporaciones privadas centralizadas que comparten información. La sigla se debe a las corporaciones integrantes las cuales son *Google*, *Apple*, *Facebook*, *Amazon* y *Microsoft* (Ramonet, 2016).

Esta "red violenta", como la llama Ignacio Ramonet, tiene la intención de que internet llegue a todo el mundo, donde no haya un rincón en el planeta que escape del acceso a internet. No obstante, la desventaja de esto es que ya no habría forma de escapar de la vigilancia masiva de estas empresas. Además, ya en la actualidad, las nuevas generaciones conviven cotidianamente con alguno o sino todos de estos servicios de internet. Asimismo, estas tienen acuerdos con más de 80 empresas de electrónica, como por ejemplo *AT&T*, *IBM*, *CSC*, *Oracle*, *Verizon*, *Motorola*, *HP*, *EDS*, *Booz Allen Hamilton* (donde trabajaba Edward Snowden previo a las revelaciones), *Qalcom*, *CenturyLink* y *Unisys* (Ramonet, 2016).

Para Ignacio Ramonet, la intención de que internet llegue a todos, es la vigilancia masiva, y tener información almacenada de todas las personas del mundo.

Además, Shoshana Zuboff describe a las acciones de las corporaciones transnacionales que almacenan datos como "capitalismo de la vigilancia", esto es recolectar experiencias como materia prima para realizar prácticas comerciales como ventas de productos y

servicios, a través de la predicción del comportamiento humano. Se plantea una ruptura de la relación entre los capitalistas y los consumidores, ya que los usuarios, no serían los consumidores, sino que sus experiencias son el producto que se vende a otras empresas (Zuboff, 2019).

Asimismo Zuboff, expone que esta práctica lleva a modificar el comportamiento a través del comercio de bienes y servicios, y que funciona con la ventaja del desconocimiento, ya que parece que acumular información fuera algo inevitable de los servicios de internet, como por ejemplo *Google*. No obstante esto no es correcto, se almacena por voluntad de la empresa y no porque sea algo que sucede por defecto cuando se usa el servicio. Delimita, además una línea entre los capitalistas y los capitalistas de la vigilancia, donde establece que los primeros al menos informan las acciones que se llevan a cabo al usar el servicio, mientras que los segundos mienten sobre el tipo de vigilancia que llevan a cabo. Destaca como capitalistas de la vigilancia a corporaciones como *Google* y *Facebook*. Google, como se ha mencionado, evita aceptar que almacenar datos sea algo que hacen por decisión propia como corporación, y Facebook plantea la vigilancia como una ventaja para el usuario. Zuboff en este caso citaba a Mark Zuckerberg, cuando él menciona que Facebook conoce todo de uno, y de sus preferencias, de este modo puede sugerirte a que bar ir cuando conoces una ciudad nueva, que se corresponda con tus gustos musicales y que el mozo te estará esperando con la bebida que te gusta.

Parece claro que el objetivo de las corporaciones es tener toda la información posible de las personas, y que puede vender esa información para que otras empresas logren vender sus productos y servicios (Zuboff, 2019).

El caso Google

Google es uno de los ejemplos y de los más relevantes, del tipo de control que tienen estas empresas sobre los usuarios.

El número de usuarios de *Google* es más de mil millones (Ramonet, 2016). Este servicio cuenta con sensores para registrar todo lo que se busca y cuando se hace. A su vez *Google Chrome* (navegador web de Google) envía a *Alphabet* (matriz de Google) todo lo que se realiza en internet, quien lo hace y en qué momento.

Además *Google Analytics* realiza estadísticas sobre las navegaciones de los usuarios en la plataforma. *Google Plus* recopila toda la información complementaria.

Con *Gmail* (también parte de *Google*) se obtienen correos electrónicos que revelan información no sólo de sus usuarios, sino también de sus contactos que incluso utilicen otro servicio de correo electrónico.

YouTube (también perteneciente a *Google*) registra las búsquedas de los usuarios, así como todo el contenido compartido por los mismos, así como sugiere material relacionado con las búsquedas previas, y emite publicidades con respecto a las mismas, predeterminado para cada usuario.

Google Maps, registra todas las localizaciones de las personas, a donde se dirigen y con qué frecuencia.

Y además de todo esto, cada *smartphone* con un sistema operativo *Android*, le hace llegar a Google todas las actividades que realice en el mismo, desde las comunicaciones, localizaciones, aplicaciones utilizadas, cuentas bancarias, compras, contactos, material audiovisual, y todo lo que llegue a hacer el usuario con el mismo.

El caso *Google*, es sólo una muestra de la información que puede obtener de los usuarios una sola de las corporaciones mencionadas.

CAPÍTULO IV

Acceso a la información: Estados y corporaciones

Alianzas

El acceso a la vigilancia masiva se da entre los Estados y las corporaciones (Ibarra, Nieves, 2016) ya que el Estado necesita contar con tecnología para tener acceso a la información y ejercer sus atributos soberanos, en otras palabras la vigilancia estatal depende de los recursos tecnológicos a los que acceda el Estado. El acceso a internet y el desarrollo tecnológico está en manos de actores transnacionales de carácter privado como son las corporaciones internacionales dedicadas a la tecnología, esto presenta un nuevo desafío para los Estados (Ibarra, Nieves, 2016). Sin embargo la cooperación entre Estados y corporaciones internacionales adquiere un nivel de vigilancia, no sólo estatal, sino que mundial (Ramonet, 2016).

Los programas detallados por Edward Snowden, no se han llevado a cabo con las tecnologías y actividades de la NSA por sí sola, sino que se ha tejido una red de alianzas que incluyen no sólo a las grandes corporaciones involucradas en el programa PRISM y en el resto de los programas, sino que también se ven influenciados por una amplia colaboración con otros Estados. Este tipo de cooperaciones no surgen con estos programas, sino que datan de largo tiempo atrás, mostrando el poder de las grandes potencias sobre los demás Estados y sobre sus propios ciudadanos (Ramonet, 2016).

En referencia al inicio de las alianzas para acceder a la información, en la segunda guerra mundial (Ramonet, 2016), ya países como Estados Unidos e Inglaterra sumaron fuerzas para descifrar códigos como *PURPLE* y *ENIGMA***.** Y ambos en 1943 realizan un acuerdo llamado *BRUSA*, con el objetivo de sentar las bases de la vigilancia masiva.

Años más tarde el acuerdo *UKUSA*, incluye a otros países, estos son, los mencionados Estados Unidos e Inglaterra, más Canadá, Australia y Nueva Zelanda. Esta alianza hoy se conoce como *FIVE EYES*, y también se conoce como la primera colaboración en materia de vigilancia masiva entre estas potencias. Asimismo en 1950, se pone en marcha la *Red Echelon*, que tiene como objetivo la intercepción de las comunicaciones.

En 1994, se lleva a cabo en Estados Unidos, una ley secreta llamada *Communications Assistance to Law Enforcement Act* (*CALEA*) que autoriza a Estados Unidos a escuchar llamadas telefónicas privadas (Ramonet, 2016).

En el programa *PRISM* además de contar con las alianzas con las grandes corporaciones de internet, *FIVE EYES* tiene un gran protagonismo y principalmente la agencia de comunicaciones de Inglaterra, la GCHQ (Poitras, 2014).

La NSA tiene documentos que son compartidos con los miembros de *FIVE EYES*, clasificados como "*FVEY"*, estos son distribuidos a sus aliados, así como también sus aliados comparten información con la NSA. Por lo que esto significa que PRISM traspasa el límite de las intenciones del gobierno de Estados Unidos, sino que además estos objetivos son compartidos con sus aliados. Sin embargo también tiene una clasificación para los archivos que no comparte con extranjeros, clasificados como "*NOFORN*" (Greenwald, 2014).

Del mismo modo, que la NSA quedó expuesta en las revelaciones de Edward Snowden, también se generó evidencia sobre las actividades de la GCHQ, que además de colaborar con la NSA, tenía su propio programa llamado *TEMPORA* con el objetivo de la vigilancia masiva.

Conjuntamente con los miembros de *FIVE EYES* - lo que en PRISM se llama el *TIER A*- existe el *TIER B*, que son otros países que comparten información sobre vigilancia masiva, estos son: Austria, Bélgica, República Checa, Dinamarca, Alemania, Grecia, Hungría, Islandia, Italia, Japón, Luxemburgo, Holanda, Noruega, Polonia, Corea del Sur, España, Suecia, Suiza y Turquía (Greenwald, 2014).

Tanto la GCHQ, como la NSA mantienen estas alianzas pagando el desarrollo de ciertas tecnologías y brindando apoyo de vigilancia a estos países (Greenwald, 2014). A su vez, Edward Snowden comenta, que incluso los aliados son objeto de vigilancia al mismo tiempo.

Estado y corporaciones

Como se ha mencionado *PRISM* cuenta con la novedad de extraer la información directamente de los servidores, es decir las grandes corporaciones de internet que funcionan en la gran mayoría del mundo. Éstas son las ya mencionadas *Microsoft*, *Google*, *Yahoo*, *Facebook*, *Skype*, *AOL* y *Apple*. Con la incorporación de estas grandes corporaciones la vigilancia en cierta forma se ha privatizado (Ramonet, 2016). La complicidad entre los Estados y las grandes empresas ha crecido, del mismo modo que la capacidad de espionaje.

Pese a esto las compañías de internet implicadas (Greenwald, 2014) alegan que solo ofrecieron a la NSA información que no era de particular importancia.

Microsoft incluso aseguró que todas las comunicaciones mediante *Skype*, eran de carácter privado, sin embargo claramente con las evidencias de Edward Snowden, esto no es cierto.

La NSA para servirse de estas compañías realizo acuerdos y negociaciones (Greenwald, 2014), no obstante la información sobre estas alianzas no es clara, ya que las corporaciones lo han negado, o han dado argumentos vagos, como el citado sobre que la información compartida no era de relevancia.

Empero, con las revelaciones de Edward Snowden se tienen pruebas de las alianzas que tienen estas corporaciones con la NSA (Poitras, 2014), y el poder que da esa información a ambas partes, como lo es la vigilancia masiva, es decir el control de todas las actividades, comunicaciones, conversaciones, localizaciones, material audiovisual, ideología, entre otros de cada uno de los ciudadanos del mundo.

Aparato que desempeña la vigilancia

La conjunción de los Estados, el aparato militar de seguridad y las grandes corporaciones de internet han generado un Imperio del que nadie puede escapar. Una nueva dimensión, el ciberespacio (Ramonet, 2016) es donde se dan las grandes interacciones y donde se encuentra la guerra por la información, en un momento en el que es de vital importancia para tener poder.

Ramonet a su vez duda de uno de los objetivos de la ONU, que es el acceso a internet para todo el mundo, ya que no quedaría nadie fuera de la vigilancia masiva (2016).

Sin duda, el poder de la vigilancia masiva trasciende incluso a la NSA, con sus aliados en otros Estados y en las grandes corporaciones.

María Gimena Rabinab también presenta el concepto de Imperio, pero como un aparato que se compone de los organismos nacionales y supranacionales. Esto se genera ya que internet revolucionó el concepto clásico de soberanía, generando discusiones entre los que considera que dejará de existir y los que creen que han mutado (Rabinab, 2008).

A lo largo de la historia la soberanía fue atribuida a un poder superior, que está por encima de todo. Se le ha atribuido la soberanía al rey, al pueblo, a la nación, pero en el

ciberespacio donde no hay fronteras no queda claro donde reside la soberanía. Esta situación estaría acompañada por cierto vacío normativo (Rabinab, 2008).

Rabinab aclara que el concepto de Imperio no debe confundirse con el de imperialismo, que este implicaba la extensión territorial de la soberanía, mientras que el Imperio opera con normas sin territorio, en las transacciones e intercambio que se dan en internet (2008).

El Imperio para Rabinab constituye los organismos nacionales e internacionales que transcienden en el ciberespacio y en la declinación de la soberanía, tomando una nueva forma. Este ¨Imperio¨ surge de la revolución en internet y las nuevas problemática, donde las instituciones tradiciones deben apartarse y mutar (2008).

En una visión liberal el internet ayuda a relacionarse internacionalmente, ya que se generan intercambios económicos entre actores no estatales, y esto lleva a un incremento de la participación de diversos países. Se van creando los espacios virtuales y van desapareciendo los reales.

Las principales discusiones con respecto al tema tienen que ver con el derecho aplicable, donde dentro de esto encontramos criterios objetivos, subjetivos, entre otros. Ésta información nos evidencia que el concepto de soberanía se ha ido transformando tomando en cuenta fenómenos como internet, sin embargo este cambio de soberanía a nivel mundial y sin fronteras, propicia una brecha entre los países de primer y tercer mundo ya que por ejemplo, en materia de propiedad intelectual, países como EEUU lograron que se tomara en cuenta su forma de proceder internamente pero hacía el exterior, como en la armonización vertical del Convenio de Berna y el Convenio GATT-TRIP. Es decir que los gobiernos negocian conflictos de internet como la propiedad intelectual pero que terminan decidiendo las potencias con poder político y económico (Rabinab, 2008).

En conclusión, el concepto de soberanía se ha modificado con los últimos acontecimientos como el de desarrollo de la tecnología e internet. Esto lleva a que surjan figuras nuevas en el ámbito internacional como lo son las corporaciones transnacionales y el concepto de Imperio ya mencionado.

CONCLUSIONES

Finalmente, se entiende que el ejercicio de los atributos soberanos del Estados se ve influenciado por el control de la vigilancia internacional en manos de corporaciones privadas, ya que las gigantes corporaciones privadas transnacionales tienen la información y tecnología adecuada para ejecutar la vigilancia con un alcance sin precedentes, esto lleva a que se construyan alianzas entre Estados y corporaciones para llevar a cabo la vigilancia internacional. Es decir que la hipótesis se cumple aunque solo se tomó un caso en particular, si bien la soberanía ha cambiado, la incorporación de internet y el avance tecnológico han hecho posible las transformaciones mencionadas, no obstante sólo se puede aplicar a EEUU en el 2013, de modo que eso no significa que la hipótesis funcione en otros casos.

Es claro que cualquier Estado no puede alcanzar este nivel de alianzas con las corporaciones e incluso con otros Estados, ya que los Estados que no tienen preponderancia internacional, es decir no tienen poder real como para presionar a una alianza no van a conseguir este tipo de acceso a la información. Esto se da en EEUU gracias a que es una potencia hegemónica. No todos pueden tener el rol que tiene EEUU hoy en día, ni su aparato de alianzas, es solo algo que pocos Estados pueden realizar, y sólo las potencias pueden alcanzar, los demás Estados quedan en una situación de desventaja ante las alianzas Estados/corporaciones, quienes imponen una forma de vigilancia a los demás, incluso en las propias alianzas donde EEUU extrae información de otros Estados que cooperan con EEUU pero a la vez son un objetivo de vigilancia.

La soberanía es un atributo esencial de los Estados independientes, aquí se manifiesta el neorrealismo, donde el Estado es el actor principal de las relaciones internacionales. Los elementos esenciales de los Estados son el territorio, la población y el poder etático, sin embargo queda demostrado que los nuevos fenómenos, como el desarrollo de la tecnología e internet, cambian estos conceptos clásicos, pues las interacciones que se realizan en internet trascienden las fronteras y las reglas internas de los Estados. De esta forma, la seguridad y la soberanía son conceptos que se han transformado. Esto constituye un nuevo orden y reglas de juego para los Estados como para las organizaciones internacionales y todo el aparato que Rabinab entiende como “Imperio”.

Dentro de las revelaciones de Edward Snowden, se destaca el programa *PRISM*, donde la NSA busca tener información sobre todo, por lo que el objetivo es global y su lema es

collect it all –recolectarlo todo-. La mayor novedad del programa, es que la información se extrae directamente de los servidores, es decir de las corporaciones implicadas (*Microsoft*, *Yahoo*, *Facebook*, *Paltalk*, *Youtube*, *Skype*, *AOL* y *Apple*), se extrae tanto la información en línea, como la receptada a través *smartphones* y computadoras, que funcionan como dispositivos de escucha, video e incluso seguimiento de localizaciones. Además la otra novedad es la alianza entre Estados y corporaciones. Lo mencionado es novedoso, principalmente para el ciudadano que se encontró con las noticias sobre el caso y que parecía una situación sacada de una película de ciencia ficción. Empero, no hay una respuesta a esa sorpresa que se llevó el ciudadano, ya que se siguen compartiendo todos los datos personales y experiencias en internet y se siguen utilizando los servicios de las grandes empresas involucradas en el programa.

La capacidad de vigilancia de las corporaciones surge de sus propios servicios en todo el mundo, ya que prácticamente todas las personas del mundo con acceso a internet poseen cuentas o utilizan alguno de los servicios de las corporaciones implicadas en *PRISM*. Para esto los usuarios comparten información por recreación, para trabajar o incluso sin un consentimiento expreso. Por ejemplo la empresa *Google*, a través de distintos servicios tiene acceso a emails, localizaciones, estadísticas de las actividades de los usuarios, búsquedas de los mismos en internet, cuentas bancarias mediante apps en *smartphones*, etc. Además su ex CEO asegura que los datos se almacenan por defecto cuando no es así, sino que se hace con un propósito.

El acceso del Estado a la información resultante del programa *PRISM*, se da por las alianzas que tiene EEUU con las corporaciones implicadas en el programa. A su vez cuenta con alianzas con otros países como Inglaterra, Canadá, Australia y Nueva Zelanda, estos países conforman lo llamado *FIVE EYES*, y con los que en el programa *PRISM* se denominan TIER B. Los países partícipes de las alianzas, asimismo, vigilan a los Estados con los que tienen alianzas.

Pese a que clásicamente el actor de las relaciones internaciones era el Estado, en el siglo XXI, las corporaciones internacionales se han convertido en un actor destacable, ya que como observamos en el PRISM, tienen la tecnología para llevar a cabo la vigilancia internacional. El ejercicio de los atributos soberanos del Estados se ven influenciados por las corporaciones ya que en el programa PRISM, el Estado debe aliarse con las corporaciones para desempeñar sus atributos soberanos como lo es la vigilancia.

Finalmente, se puede decir que en este caso que el concepto de soberanía cambia a una soberanía sin fronteras, pero que a la vez acrecienta la brecha entre el primer y el tercer mundo, ya que las normas que rigen al ¨Imperio" son negociadas e implementadas por las grandes potencias. De todas formas pese a la influencia de la vigilancia de las corporaciones internacionales y la mutación en el concepto de soberanía en el caso planteado el Estado tiene aún un rol vital en esta relación y teniendo en cuenta sus respectivas alianzas. No obstante esto no se puede probar en el resto de los Estados, que pueden ser capaces o no, de generar alianzas de tal magnitud, y podríamos plantearnos a futuro si en otros casos las corporaciones tienen más control de los atributos soberanos que los propios Estados.

También se puede retomar la teoría neorrealista, ya que se puede ver que los actores en este tema, deciden teniendo en cuenta sus distintos intereses. Edward Snowden, quien siente que tiene un peso muy grande conociendo esta información y no compartirla con los demás ciudadanos, termina cediendo ante su ética (que está relacionada con la ética hacker) y robando los datos sobre PRISM para ser publicados. A su vez, el gobierno de EEUU debe mantener su rol preponderante a nivel mundial y para eso debe contar con información y tecnologías para estar en un lugar de ventaja a nivel mundial. Sin embargo, los perjudicados con todo esto son los ciudadanos ya que no deciden sobre que compartir y que no compartir, o cuando deciden desconocen del tema, como planteaba Zuboff, cuando dice que los capitalistas de la vigilancia tienen a favor el desconocimiento de los ciudadanos, ya que les dicen que los datos se guardan por defecto, cuando no es así, de manera que el comportamiento de los ciudadanos se convierte en una moneda de intercambio.

Referencias bibliográficas

Esnal, G., Ibarra, V., Jackson, M., Messano, F., Nieves, M., y Sabiguero, A. (2016) Relaciones entre la soberanía y tecnología en los tiempos de internet. Revista de la Facultad de Derecho. No. 41. pp. 259-286.

Greenwald, G. (2014) No place to hide: Edward Snowden, the NSA, and the US surveillance state. New York: Picador.

Harding, L. (2014) The Snowden Files. New York: Vintage books.

Ibarra, V. y Nieves, M. (2016) La seguridad determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. Universidad Nacional de la Plata. Facultad de Ciencias Jurídicas y Sociales.

Moller, B. (1996) Conceptos sobre seguridad: Nuevos riesgos y desafíos. Desarrollo económico. Revista de Ciencias Sociales. Vol. 36. No. 143. pp.769-792.

Olmedo González, H. (2013) Tradiciones de investigación y teorías en el estudio de las relaciones internacionales. Universidad de la República, Facultad de Ciencias Sociales. Serie documentos de trabajo no. 81.

Orozco, G. (2006) El aporte de la Escuela de Copenhague a los estudios de seguridad. Universidad Autónoma de Madrid: Revista de Fuerzas Armadas y Sociedad. Año 20. No. 1 pp.141-162.

Osaba, J. (2015) La distopía ya está aquí: Vigilancia estatal de Orwell a Snowden y El Guardían. Revista Dixit no.23. Julio –Diciembre pp.05-15.

Pilnik, F. (2017) Delitos en el ciberespacio. Córdoba: Advocatus.

Rabinab, M. (2008) La soberanía del ciberespacio. Lecciones y ensayos no.85 pp. 85-107.

Ramonet, I. (2016) El Imperio de la Vigilancia. Buenos Aires: Clave Intelectual.

Salomón, M. (2002) Las teorías de las Relaciones Internacionales en los albores del siglo XXI: Diálogo, disidencia y aproximaciones. Revista electrónica de estudios internacionales.

The Wikileaks Files (Anónimo, 2015) New York: Verso.

Verdes-Montenegro Escánez, F. (2015) Securitización: agendas de investigación abiertas para el estudio de la seguridad. UAM: Relaciones Internacionales. No. 29 pp.111-131.

Zuboff, S. (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs.

Filmografía

Bloom, A., Gibney, A., Shmuger, M. (productores) y Gibney, A. (director) (2013) We steal secrets: The story of wikileaks (documental). US: Jigsaw Productions y Global Produce.

Bonnefoy, M., Poitras, L., Wilutzky, D. (productores) y Poitras, L (directora). (2014) Citizenfour. US-DE: HBO Films, Participant Media y Praxis Films.

Borman, M., Kopeloff, E., Schulz-Deyle, P., Sulichin, F. (productores) y Stone, O. (director). (2016) Snowden. US-DE: Endgame Entertainment, KrautPack Entertainment, Onda Entertainment, Vendian Entertainment y Wild Bunch.