Protección Internacional de la Privacidad y Regulación del Uso de Datos Personales, ¿una Utopía?: Análisis del Caso de Estados Unidos en la Era Posterior a las Revelaciones de Edward Snowden

Pontificia universidad javeriana

Facultad de Ciencias Políticas y Relaciones Internacionales

Relaciones Internacionales

Bogotá D.C.

2023

Protección Internacional de la Privacidad y Regulación del Uso de Datos Personales, ¿una Utopía?: Análisis del Caso de Estados Unidos en la Era Posterior a las Revelaciones de Edward Snowden

Sahian Manuela Mora Piñeros

Pontificia universidad javeriana

Facultad de Ciencias Políticas y Relaciones Internacionales

Relaciones Internacionales

Bogotá D.C.

2023

Tabla de Contenido

Lista de figuras

Lista de abreviaturas

Recuento de las abreviaciones utilizadas en el presente trabajo de grado, organizadas por orden alfabético.

- **CIA** – Agencia Central de Inteligencia, de su nombre original en inglés *Centra Intelligence Agency*
- **FBI –** *Federal Bureo of Investigation*
- **FISA –** *Foreign Intelligence Surveillance Act*, o Ley de Vigilancia de Inteligencia Extranjera.
- **FISC –** *Foreign Intelligence Surveillance Court,* o Tribunal de Vigilancia de Inteligencia Extranjera.
- **GDPR –** Regulación General de Protección de Datos, o General Data Protection Regulation
- **NSA –** Agencia de Seguridad Nacional, de su nombre original en inglés *National Security Agency*
- **ONU –** Organización de Naciones Unidas

Planteamiento del Problema

Edward Snowden, alias Verax

Edward Joseph Snowden es uno de los hombres más conocidos de la historia reciente. Su caso trascendió fronteras y se volvió un hito en la discusión sobre uso de datos, privacidad, espionaje y seguridad nacional. Tras años de trabajo en el área de seguridad informática para distintas instituciones del gobierno estadounidense, el programador se dio a conocer al revelar una serie de documentos que daban cuenta del alcance y sofisticación de los programas de espionaje del gobierno (Hagan, 2022).

Snowden nació en 1983 en Elizabeth City, Carolina del Norte. En la década de los 2000 dio sus primeros pasos en las áreas de tecnología y computación y hacia finales de 2004 consiguió trabajo como guardia de seguridad en Centro de Estudios Avanzados del Lenguaje de la Universidad de Maryland, una instalación perteneciente a la red de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). Poco después fue contratado por la Agencia Central de Inteligencia (CIA, por sus siglas en inglés) como ingeniero de sistemas y computación, en el área de seguridad de tecnologías de información (Hagan, 2022).

Durante años sus distintas asignaciones como empleado y contratista tanto de la NSA como de la CIA le dieron a Snowden acceso a información confidencial sobre los programas de espionaje masivo de las instituciones gubernamentales de seguridad nacional; programas de envergadura tal, que permitían al gobierno rastrear y acceder a correos electrónicos y llamadas telefónicas de ciudadanos comunes en todo el territorio nacional y más allá de sus fronteras (Hagan, 2022).

Consciente de las implicaciones y el alcance de estos programas, Snowden utilizó sus accesos para descargar una gran cantidad de documentos clasificados que daban cuenta del espionaje gubernamental. Lejos del país y con las pruebas en su poder, el programador contactó a Laura Poitras, una realizadora independiente y al escritor Glenn Greenwald, con quienes – bajo el pseudónimo Verax – organizó la filtración y revelación de los documentos al público en dos de los medios más importantes del mundo: *The Guardian* (Reino Unido) y *The Washington Post* (Estados Unidos) (Hagan, 2022). El

primer documento fue publicado por *The Guardian* el 6 de junio de 2013, y de ahí en adelante se desató uno de los más álgidos debates sobre seguridad nacional, privacidad y uso de datos en la era contemporánea.

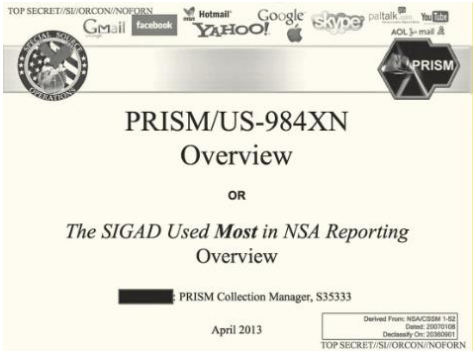
Barton Gellman, reportero que trabajó de la mano con Laura Poitras en la divulgación de los documentos, describió así el momento en el cual vio por primera vez el contenido de estos:

> Los puntos principales fueron muy claros. Bajo el nombre de PRISM, la NSA estaba desviando datos de decenas de miles de cuentas de Yahoo!, Google, Microsoft y Facebook, entre otras. Cuarenta y una diapositivas y 8.000 palabras de notas del orador expusieron los fundamentos jurídicos y los detalles de funcionamiento. Si es auténtico -y sin duda lo parece-, este informe ofrece algo muy raro: una descripción autorizada, casi en tiempo real, de las operaciones de inteligencia en suelo estadounidense que se extendieron mucho más allá de los límites reconocidos en público[1]. (Gellman, Secrets, Sirveillance and Snowden, 2020, pág. 103)

Efectivamente, una de las revelaciones más determinantes fue el programa PRISM que permitía a la NSA acceder a los sistemas de las principales compañías tecnológicas para sus esfuerzos de vigilancia, recolectando todo tipo de información personal de los usuarios. La imagen expuesta a continuación es la portada del documento relacionado con este programa, entregado por Snowden a sus colaboradores periodistas (Gellman, Secrets, Sirveillance and Snowden, 2020).

Figura 1

Portada de los documentos filtrados sobre el programa PRISM



Fidler, D. P. (2015). *The Snowden Reader*. Bloomington, IN: Indiana University Press. PP-102

[1] Traducción propia de la versión original en inglés.

El mismo Gellman (2020) recuerda la justificación que Snowden, aún bajo su pseudónimo Verax, le dio a él y a Poitras para explicar sus acciones. ¿Por qué un reputado miembro de la comunidad de inteligencia de Estados Unidos decidía arrojar su vida y carrera por la borda con la revelación de secretos de Estado? Según Gellman (2020), Snowden señaló lo siguiente[2]:

> Mi único motivo es informar al público de lo que se hace en su nombre y de lo que se hace contra él. El gobierno de Estados Unidos, en conspiración con Estados clientes, el más importante de ellos el denominado Cinco Ojos – conformado por Reino Unido, Canadá, Australia y Nueva Zelanda- han infligido al mundo un sistema de vigilancia secreta y omnipresente del que no hay refugio. Protegen sus sistemas nacionales de la vigilancia de los ciudadanos mediante la clasificación y las mentiras, y se protegen de la indignación en caso de filtraciones haciendo demasiado hincapié en las limitadas protecciones que deciden conceder a los gobernados. Les digo por experiencia que estas protecciones pueden ser despojadas en un instante.

Las partes involucradas sabían el riesgo que corrían. La revelación de esta información supondría una persecución decidida por parte del gobierno e, incluso, por parte de los servicios de inteligencia de otros Estados. Snowden, quien se encontraba en Hong Kong al momento de la primera filtración (Hagan, 2022), entendía las implicaciones, pero se mantuvo firme: "La mejor de las suertes en su reportería – Que la verdad sea conocida"[3], dijo a Gellman (2020). A partir de ese momento se desató la tormenta.

El 9 de junio del mismo año, el mismo Snowden hizo público que había sido él el informante que filtró los documentos, dando pie al Departamento de Justicia de Estados Unidos a abrir una indagación penal en su contra por tres delitos: robo de propiedad gubernamental, revelación de información clasificada y transferencia de documentos clasificados a partes no autorizadas (Hagan, 2022). El gobierno falló en su intento de acordar con Hong Kong la extradición del informante, quien terminó huyendo a Rusia el

[2] Traducción propia de la versión original en inglés.
[3] Traducción propia de la versión original en inglés.

23 de junio. El impacto de los acontecimientos sobre la opinión pública fue tal, que la revista Time nombró a Snowden "Personaje del Año"[4] en 2013, el año de las revelaciones.

Rusia mantuvo a Snowden bajo asilo político desde 2013 hasta 2020, año en el cual le concedió la ciudadanía rusa. Durante estos años, el programador ha dado varias conferencias virtuales desde locaciones secretas y se ha convertido en uno de los hombres más relevantes en el escenario político reciente. Como señala David Fidler, "la publicación de documentos clasificados por parte de Snowden tuvo una importancia trascendental por las cuestiones políticas, jurídicas y éticas que planteó en Estados Unidos y en todo el mundo" (Fidler, 2015, pág. 12).Tras la publicación de su libro, *Vigilancia Permanente*, en 2019, Snowden ha continuado activo en el debate público sobre la privacidad y el espionaje gubernamental en la actualidad (Hagan, 2022).

La libertad individual y el derecho a la privacidad

Como indica Fidler (2015, pág. 19) "Si un tópico capta el tenor del debate en torno a las revelaciones de Snowden, es la metáfora recurrente del equilibrio entre libertad y seguridad"[5]. ¿Hasta qué punto llega la libertad del individuo, cuando se entra en el terreno de la seguridad nacional? Este debate se ha presentado en otros momentos de la historia; sin embargo, el caso Snowden lo revive en una época donde la tecnología, el big data y la transformación digital están en auge. Como señala el mismo autor:

> Las revelaciones de Edward Snowden sobre la vigilancia de la Agencia de Seguridad Nacional han dominado la actualidad mundial como pocos acontecimientos en los últimos años. Héroe para algunos y traidor para otros, sus revelaciones desataron, como él esperaba, un debate mundial sobre la vigilancia estatal en el contexto de los avances tecnológicos, cuyas implicaciones la mayoría de los formuladores de política, por no hablar de los ciudadanos de a pie, apenas alcanzan a comprender (Fidler, 2015, pág. 70).

El caso Snowden está definido en particular por el alcance y la dimensión de las técnicas de vigilancia estatal que fueron reveladas. En palabras de Greenwald (2017) la

[4] "Person of the Year" en idioma original.
[5]Traducción propia de la versión original en inglés.

intensidad del debate en torno a este caso y su permanencia en el tiempo se debe a que el debate desencadenado por estas revelaciones de hecho terminó siendo sobre mucha más que solo vigilancia:

> Por primera vez se ha producido a nivel mundial un profundo examen de lo que significa la privacidad individual en la era digital y por qué es importante. Se ha producido un serio debate sobre los peligros de dotar a los grandes gobiernos de un inmenso poder, que pueden ejercer en la oscuridad sin transparencia ni responsabilidad real (Greenwald G. , 2017, pág. 35).

Esto nos lleva a considerar un concepto clave dentro de esta discusión: la privacidad. Como indican Brenner & Clarke, "ha habido siempre una estrecha relación entre la tecnología y el reconocimiento en el sistema legal del derecho a la privacidad" (pág. 5). En la actualidad, con los flujos masivos de datos y nuevas realidades informáticas, como la realidad virtual y los primeros pasos del metaverso, que diluyen las fronteras de lo físico, el concepto de la privacidad enfrenta retos mayores y debe ajustarse.

Hoy en día la ciudadanía – en lo que podría parecer una materialización de la distopía de Orwell en 1984 – se ha hecho cada vez más consciente de que su información está expuesta, "no solo de forma perversa, sino, además, inevitable" (Brenner & Clarke, 2007, pág. 6). Entre más avance la tecnología, más difusa se hará la barrera entre aquello que es privado, y aquello que no lo es, y la información de las personas será rastreada, recolectada y utilizada sin que la regulación orientada a establecer límites logre seguirle el ritmo.

Como señala Bass (2019):

> En la actual economía global de la información, interconectada y dependiente de Internet, los consumidores divulgan voluntariamente, pero a menudo sin saberlo, sus datos personales y privados a las empresas tecnológicas, con frecuencia sin tener en cuenta su custodia o su uso futuro. (Bass, 2019, pág. 261).

En este mismo sentido, Greenwald señala que en un mundo digital como el que tenemos, en el cual la privacidad está desapareciendo, es un mundo en el cual los

individuos son conscientes de que cada cosa que hagan es susceptible de ser monitoreada por las autoridades, un mundo "en el cual la libertad humana ha sido reducida dramáticamente y de forma fundamental" (Greenwald G. , 2017, pág. 47).

De hecho, las revelaciones de Snowden dieron paso a un escenario en el cual el Estado tuvo que empezar a hablar de sus verdaderas capacidades en materia de vigilancia; Estados Unidos tuvo que afrontar la discusión sobre el alcance de sus instituciones de seguridad nacional, y así se dio el primer paso para debatir cuál es la forma de controlar esas capacidades (Sanger, 2017).

Con sus revelaciones, Snowden "abrió los ojos del mundo a un nuevo mundo de vigilancia y ciberguerra. Lo que reveló no puede volver a meterse en una caja negra, y cambiará la forma en que vemos el poder estadounidense en la próxima década" (Sanger, 2017, pág. 196).

En este contexto, se eleva la discusión sobre el efecto que el uso de los datos personales por parte de actores como el Estado, puede tener sobre los derechos individuales. Como argumenta Giacomello (2014) en la introducción de su libro sobre seguridad en el ciberespacio, los beneficios que el Internet ofrece pueden constituir una amenaza; la novedad de la tecnología y la ausencia de una gobernanza uniforme sobre el ciberespacio han abierto la puerta a prácticas que pueden caer en la violación de los derechos humanos (Giacomello, 2014).

En suma, parte de lo que llevó al caso Snowden a ser un hito de nuestro tiempo fue el impacto que causó en la opinión pública empezar a dimensionar los alcances del Gobierno en materia de recolección de datos. En palabras de Fidler (2015) la revelación de Snowden:

> Avergonzó al gobierno estadounidense, despertó miedos sobre el daño a la seguridad nacional, desató controversias sobre el posible abuso contra las libertades civiles en Estados Unidos, enfureció a los ciudadanos y a los líderes de países extranjeros, incluyendo a aliados de Estados Unidos, quienes descubrieron que la NSA tenía acceso a sus comunicaciones. (Fidler, 2015, pág. 12).

Como se ha mencionado, si bien los debates sobre privacidad, seguridad nacional y vigilancia no son nuevos, la irrupción de la interconexión digital, las redes sociales y otros múltiples canales a través de los cuales los individuos pueden exponer su información personal han cambiado la escala de esos debates (Unver, 2018). Así:

> La rápida evolución de las tecnologías crea un sistema en el que la información personal digitalizada y los datos oficiales tienen ahora múltiples puntos de interceptación, no pueden borrarse de forma fiable, no caducan y pueden difundirse por las plataformas digitales a un ritmo infinito y a una velocidad vertiginosa (Unver, 2018, pág. 2).

Las acciones de Snowden en 2013, sumadas al contexto tecnológico y de información del momento, lo convirtieron en una de las figuras más importantes y polémicas en la discusión global sobre privacidad, vigilancia estatal y uso de datos, y las repercusiones de estas se sienten hasta el día de hoy.

USA Freedom Act: regulación de la recolección de datos personales por parte del gobierno

En verano de 2015, dos años después de la primera filtración de Snowden en *The Guardian*, se adoptó la ley conocida coloquialmente como "USA Freedom Act"[6] o Ley de Libertad Estadounidense. El nuevo texto, que reformaba el *USA Patriot Act* (a su vez, reforma del *Foreign Intelligence Vigillance Act* de 1978), buscaba implementar modificaciones a las condiciones bajo las cuales las autoridades estadounidenses recolectaban datos telefónicos y de internet de los ciudadanos, limitando el margen de maniobra de instituciones como la NSA.

Con las revelaciones de Snowden, la confianza pública en las instituciones se deterioró considerablemente y esta ley fue vista como el intento de parte del gobierno y el Congreso de recuperarla. En palabras de Berman (2016) el caso Snowden provocó un cambio significativo en la noción pública sobre las actividades gubernamentales de vigilancia y abrió paso a la oportunidad de reforma; este proceso culminó – al menos en una primera etapa – en la aprobación del USA Freedom Act.

[6] Se conserva el nombre en inglés en algunas ocasiones.

Como se ha visto, las revelaciones de Edward Snowden marcaron un momento significativo en el debate sobre privacidad, tecnología, manejo de datos personales y muchos otros aspectos. Si bien no ha sido el único caso en motivar este debate, sí es uno de los más relevantes por sus recientes implicaciones políticas, éticas y de seguridad nacional, no solo en Estados Unidos sino en el mundo entero. Las revelaciones de Snowden dejaron en evidencia no solo la existencia (que ya se conocía) de programas de vigilancia estatal, sino el alcance y la escala que esos programas habían alcanzado: se podía vigilar de forma masiva, "preventiva" y en tiempo real, prácticamente en cualquier parte del mundo.

Ausencia de un régimen internacional de protección de datos

Teniendo esto en cuenta, llama la atención que – hasta el día de hoy[7] – no existe a nivel global un régimen sobre privacidad y protección de datos personales. A pesar del impacto del caso Snowden y de otros similares como WikiLeaks, los continuos debates sobre esta materia no han logrado dar como resultado una herramienta jurídica vinculante que regule la recolección y el uso de datos por parte de los Estados a nivel internacional. Esto, incluso considerando que, a medida que la capacidad de las herramientas digitales y tecnológicas se profundiza, la capacidad de individuos y Estados de controlar los flujos masivos de datos, y la huella digital de la información, se reduce aceleradamente.

Pregunta de investigación

El presente trabajo de investigación se propone responder la siguiente pregunta: **¿Cómo se explica la modificación de la legislación sobre privacidad y protección de datos en Estados Unidos, específicamente a través del Freedom Act de 2015, en el contexto posterior a las revelaciones de Edward Snowden?**

[7] Escrito en octubre de 2022.

Objetivos

Objetivo General

Dar cuenta de la modificación de la legislación sobre privacidad y protección de datos personales en Estados Unidos, específicamente a través del Freedom Act de 2015 en el contexto posterior a las revelaciones de Edward Snowden.

Objetivos específicos

- Analizar las revelaciones de Edward Snowden y situarlas en el problema que se plantea sobre privacidad, vigilancia estatal y uso de datos.
- Dar cuenta del surgimiento del Freedom Act de 2015, sus implicaciones y su contexto tras a las revelaciones de Edward Snowden.
- Analizar los acontecimientos expuestos a la luz de los planteamientos teóricos del institucionalismo neoliberal y la interdependencia compleja.

Justificación

El presente trabajo de investigación aborda varios temas que son de relevancia para la disciplina de relaciones internacionales. En esta sección se exponen brevemente los argumentos que justifican la necesidad de abordar el tema de estudio, y de continuar explorando sus ramificaciones dentro de la academia.

El acelerado avance que ha tenido Internet durante los últimos años ha determinado la forma de relacionarse de los sujetos, no únicamente en lo que respecta a individuos, sino trascendiendo a la interacción entre los Estados, corporaciones y personas. Dentro de la relación que se tiene con este nuevo entorno digital se encuentra la recopilación y almacenamiento de datos, un proceso automatizado que llevan a cabo las empresas digitales.

El acceso a esos datos es un elemento de poder. En el caso de los Estados, el denominado *ciberpoder* tiene una importancia enorme en el contexto actual, por lo cual los gobiernos de todo el mundo están desarrollando nuevas capacidades, diseñando estrategias y explorando el uso del poder en el ciberespacio (Voo, Hemani, & Cassidy, 2022).

De acuerdo con la definición que hace el proyecto *National Cyber Power Index*, el ciberpoder debe entenderse desde una perspectiva amplia en la cual:

> Los Estados buscan no sólo destruir e inutilizar la infraestructura y las capacidades del adversario (la percepción tradicional, pero estrecha y engañosa, del poder cibernético), sino también reforzar y mejorar las ciberdefensas nacionales, reunir información de inteligencia en otros países, aumentar la competencia nacional en materia de tecnología cibernética y comercial, controlar y manipular el entorno de la información, y ampliar su influencia mediante la definición de normas cibernéticas y estándares técnicos internacionales (Voo, Hemani, & Cassidy, 2022, pág. 2).

Por el lado de las empresas, está el concepto del capitalismo de vigilancia – *Surveillance Capitalism* – que se refiere a la práctica económica de acumular y vender información de los consumidores, en muchas ocasiones sin su conocimiento o consentimiento (Biscontini, 2021). Las compañías descubrieron lo que Zuboff (2019) denomina el "excedente de conducta" (behavioral surplus): formas nuevas de usar los datos de los usuarios para otros propósitos distintos a los de mejorar los servicios y productos que ofrecen. Así, el sector privado recolecta y vende masivamente la información de sus usuarios, con los casos emblemáticos de Google y Facebook.

Así las cosas, y como se ha mencionado, los patrones de flujo de información son uno de los factores más importantes que dan forma al fenómeno de la globalización. Hoy en día los individuos, así como los Estados y otros actores internacionales, están intentando controlar los vastos flujos de información que atraviesan fronteras y que elevan una nueva discusión sobre el poder (Subramanian & Katz, 2011). En el contexto actual, gracias al Internet – el mayor habilitador de la globalización – las empresas, las organizaciones y, especialmente, la sociedad civil, están en posición de poder influenciar a los gobiernos y, por extensión, al sistema internacional (Drezner, 2011).

De hecho, en palabras de Subramanian & Katz (2011), los entornos digitalmente interconectados someten la información a métodos nunca vistos de manipulación y distribución, y los conflictos sobre esos flujos de información son ahora una condición fundamental para definir quién tiene poder sobre la economía global de la información.

Este es sin duda un escenario retador para el estudio de las relaciones internacionales. Es en este contexto que se presenta el caso seleccionado para esta investigación: las revelaciones de Edward J. Snowden. Este caso es relevante para la academia y para la política internacional porque tuvo un impacto importante sobre aspectos sociales (debate público), regulatorios (nuevas leyes y modificaciones regulatorias en varios Estados), políticos (crisis de la definición de seguridad nacional, deterioro de relaciones entre Estados, desconfianza) y éticos (discusión sobre los límites del Estado y la vulneración de los derechos individuales). A raíz de esto, el caso Snowden ha sido analizado desde diversas perspectivas, desde la de seguridad y el Estado de vigilancia (Gellman, 2020), hasta estudios de comunicación, periodismo y medios (Khorana, Henrichsen, Bell, & Owen, 2017). Este trabajo en particular pretende darle una mirada desde la noción de instituciones y regímenes internacionales, y desde los derechos humanos. La protección de los derechos humanos es un régimen que se ha normalizado en el sistema, y que ha ido robusteciéndose con los años.

Sin embargo, el caso Snowden reveló que la actuación del gobierno estadounidense había excedido los límites de la privacidad como derecho individual consignado en la Declaración Universal de Derechos Humanos, y, hasta cierto punto, puso en duda la validez y pertinencia del régimen a nivel global. ¿Hasta dónde puede llegar el Estado cuando se trata de proteger la seguridad nacional? ¿Qué implicaciones tienen estas revelaciones sobre la concepción de los derechos individuales? ¿Cómo respondieron los Estados ante esta coyuntura que trascendió fronteras? ¿Cómo se interpreta este caso a la luz de la declarada guerra contra el terrorismo derivada de los ataques del 9-11? Todas estas son cuestiones importantes que se pueden – y deben – abordar desde el estudio de las relaciones internacionales.

Este caso eleva una preocupación en torno a la protección de los datos personales y deja en evidencia la alta vulnerabilidad que, como el mundo globalizado, enfrenta día a día, considerando que es imposible vivir fuera de ese sistema y que la existencia humana actualmente se encuentra permeada por las nuevas tecnologías. Este estudio busca analizar la interdependencia que existe entre actores no estatales y estatales, no solo a nivel doméstico sino también en el sistema internacional, y las repercusiones (o ausencia de ellas) de un acontecimiento específico dentro de un Estado; además pretende utilizar teorías de la década de los 70 para analizar un fenómeno muy actual, y así mostrar la

validez de estas y su aplicabilidad en un contexto de hiper conectividad, globalización y revolución digital acelerada.

Marco metodológico

Enfoque relacional como aproximación general de investigación cualitativa

El presente trabajo de investigación pretende, como se ha mencionado, dar cuenta de la modificación de las leyes sobre privacidad y protección de datos en Estados Unidos, específicamente el USA Freedom Act de 2015, que se desarrolló en el contexto posterior a las revelaciones de Edward J. Snowden sobre los programas gubernamentales de espionaje en manos de las instituciones de seguridad nacional.

Para ello, es necesario establecer no solo las herramientas sino la posición metodológica de la autora de este trabajo. Como señala Howard (2010): "la meta de la metodología no es resolver los debates intelectuales preexistentes, sino más bien partir de una posición particular y articular qué exactamente "cuenta" como conocimiento" (pág. 394). Este marco metodológico pretende establecer cómo se dará sentido al caso seleccionado y a la información recolectada en el proceso de investigación.

De acuerdo con Howard (2010), en la disciplina de las relaciones internacionales, existen tres aproximaciones o enfoques metodológicos dominantes: el enfoque neopositivista, el enfoque interpretativo y el enfoque relacional. El presente trabajo de investigación se enmarca en este último.

Cada uno de los enfoques expuestos por Howard (2010) tiene una triangulación de posiciones distintas sobre tres debates fundamentales: la causalidad, el contexto y la esencia. A continuación, se describe brevemente el argumento del autor en torno a esos tres debates.

El debate sobre la *causalidad* se da entre aquellos académicos de la disciplina que rechazan la noción de una "causa" para explicar el mundo social, y aquellos que – por el contrario – ven la "causa" como el centro de la explicación de un fenómeno determinado. Adicionalmente, este último grupo se divide en dos: quienes defienden la existencia de una causalidad general, y quienes se inclinan por hablar de causalidad particular o específica (Howard, 2010).

Por su lado, el debate sobre el *contexto* es el que se centra en el rol del contexto social en la ciencia. En este punto, hay académicos que defienden la irrelevancia del contexto en la explicación del funcionamiento del mundo observable; en la orilla contraria están los académicos que consideran que el contexto no solo importa, sino que es tan rico y complejo que es imposible diseccionarlo en variables objetivas.

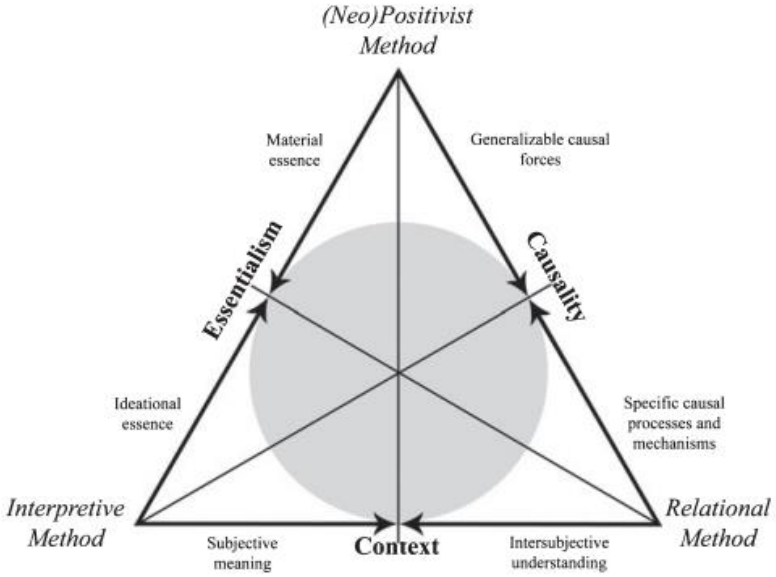
Cuando el investigador parte de la base de que el contexto es relevante, se pasa a la pregunta que subdivide dos grupos más: ¿el significado de un contexto es completamente subjetivo, determinado por el observador de forma individual, o más bien es intersubjetivo, creado por comprensiones colectivas entre actores sociales? Así, el contexto bien puede ser irrelevante, subjetivo o intersubjetivo. (Howard, 2010)

Finalmente, está el debate sobre la *esencia o esencialismo*. La visión esencialista es la que defiende que los actores u objetos tienen una esencia clara, identificable y estática. En contraposición, están quienes señalan que todos los actores y fenómenos deben ser considerados como procesos y no como cosas; la denominada esencia de una "cosa" es un producto específico de un proceso en determinado momento y su aparente "quietud" se puede explicar a través de ese proceso (Howard, 2010).

La distinta combinación de posiciones con respecto a estos tres debates da como origen tres aproximaciones metodológicas distintas. El autor presenta el siguiente esquema para visualizar su propuesta de triangulación (Figura 2).

Figura 2

Triangulación de debates fundamentales y aproximaciones metodológicas[8]



Howard, P. (2010). Triangulating Debates Within the Field: Teaching International Relations Research Methodology. *International Studies Perspectives*, 393-408

Para efectos del presente trabajo solo se profundizará en el enfoque seleccionado: el relacional. De acuerdo con Howard (2010) esta aproximación es un ejemplo del impacto de la sociología relacional sobre la disciplina de relaciones internacionales que, con respecto a los debates fundamentales mencionados, parte de los siguientes supuestos:

a) **La causalidad es un proceso:** es el resultado de mecanismos específicos actuando de forma específica y produciendo un resultado particular e identificable. Los resultados no son generalizables porque dependen de las circunstancias, y las variaciones no pueden ser comprendidas por fuera del contexto. En palabras del autor, en lugar de preguntarse por la causa de la guerra, "un enfoque de mecanismos causales sugiere preguntar qué causo una guerra particular, o, más bien, cómo un grupo de mecanismos causales llevaron al estallido de la guerra en cuestión" (Howard, 2010, pág. 397).
b) **El contexto es relevante y el significado es intersubjetivo**: esto quiere decir que el sentido o significado es un conjunto de acuerdos o nociones colectivas. No se

[8] Tomado de: Howard, P. (2010). Triangulating debates within the field: teaching international relations research methodology. *International Studies Perspectives*, 393-408.

trata de lo que un individuo cualquiera crea o interprete; el significado se encuentra en lo que un grupo humano comparte y racionaliza de forma colectiva (Howard, 2010). Además, hay un aspecto clave que el autor destaca y es que, desde la perspectiva intersubjetiva, el contexto social puede ser mantenido durante un tiempo determinado, permitiendo que se desarrollen y estabilicen formas sociales complejas, pero no está determinado y no es indiferente a las presiones de cambio.

c) **Los fenómenos sociales han de ser interpretados como procesos, y no como cosas: "**los actores son producto de prácticas constitutivas en curso" (Howard, 2010, pág. 399). Desde esta perspectiva, el trabajo del investigador es desglosar las "cosas" en los procesos que le dieron forma, y explicar el cambio como un proceso que llevó a un resultado distinto, en una coyuntura o situación particular.

Así las cosas, en enfoque metodológico relacional delineado por Howard (2010) se caracteriza por rechazar el esencialismo y enfocarse en los procesos causales y sus especificidades, así como en la naturaleza intersubjetiva y relevante del contexto social. "Un diseño de investigación relacional busca identificar ya sea la constitución de entendimientos intersubjetivos y tejidos sociales, o los procesos causales que crean, mantienen o modifican esos entendimientos" (Howard, 2010, pág. 401). El autor continúa señalando que "el resultado de esta investigación es un recuento de cómo se presentó una configuración particular de procesos sociales para producir un resultado significativo e identificable" (Howard, 2010, pág. 401).

Esta aproximación es adecuada para el presente trabajo de investigación, por varias razones. En primer lugar, este texto busca entender el grupo de mecanismos causales que llevó a lo que Howard (2010) llama un resultado específico e identificable, en este caso, la promulgación de la ley USA Freedom Act en 2015, en Estados Unidos. Se intentará tejer la causalidad de un proceso que dio origen a un resultado observable y específico.

En segundo lugar, están el contexto y la intersubjetividad. Este trabajo considera que es justamente el contexto el que da sentido a la causalidad que deriva en el Freedom Act de 2015; un contexto de desconfianza y presión por parte de la opinión pública, derivada de las revelaciones de Edward J. Snowden en 2013. Desde la perspectiva

intersubjetiva, el contexto de Estados Unidos en el cual había un fuerte sentimiento nacionalista, un temor generalizado a posibles ataques terroristas tras los eventos de 11-S, y un fuerte apoyo a la protección de la seguridad nacional parecía bien fundado, pero no fue indiferente ante las presiones de cambio.

En últimas, lo que se pretende con esta investigación es "desglosar" el Freedom Act de 2015 (objeto o resultado identificable) en los procesos que le dieron forma y, además, explicar ese cambio en Estados Unidos como un proceso que – en el contexto post-Snowden – llevó a un resultado específico.

Estudio de caso

Este método es uno de los más conocidos, no solo dentro de la disciplina de relaciones internacionales, sino en general en la investigación cualitativa. Como señalan Goertz & Mahoney (2012) "en la investigación cualitativa hay siempre un mayor foco en eventos específicos y en procesos que tienen lugar dentro de cada caso individual" (pág. 87).

El método de *estudio de caso* examina un caso en detalle, empleando múltiples fuentes de datos. El caso puede ser seleccionado por su particularidad o carácter único, o bien por su repetición constante y su delimitación depende del investigador" (Range, 2021). Para aplicar este método se deben seguir varios pasos: definición del universo de casos posibles, selección del caso que sea más adecuado conforme a la investigación, desarrollo y comparación, ya sea interna o externa (Klotz, 2008).

Para el interés general de la presente investigación, la modificación de la ley estadounidense sobre privacidad y uso de datos, se podrían definir varios casos de estudio. En primer lugar, están las diversas leyes que componen el marco legal sobre este tema en Estados Unidos, entre las que se cuentan, según Heisenberg (2005), las siguientes: el *Fair Credit Reporting Act* de 1970 y su posterior modificación en 1992, el *Privacy Act* de 1974, el *Family and Education Rights and Privacy Act* del mismo año, el Right to Financial Privacy Act de 1976, el Privacy Protection Act de 1980, el *Telecommunications Act* de 1996, el *Children's Online Privacy Protection Act* de 1998, y el Freedom Act de 2015, entre otras.

Todos estos son posibles casos de estudio para indagar sobre la legislación de Estados Unidos en materia de datos y privacidad, y su modificación. Sin embargo, como fue señalado en el planteamiento de esta investigación, el Freedom Act de 2015 fue consecuencia de un contexto clave en los años recientes: las revelaciones de Edward Snowden. Si bien no es el único momento de la historia donde se ha desatado una discusión pública sobre el tema de la privacidad, sí se puede afirmar que el caso Snowden es uno de los más recientes y de mayores dimensiones, precisamente por darse en la época de big-data y revolución digital acelerada. Sus impactos trascendieron al escenario de la opinión pública y pasaron a la legislación, a la política exterior de Estados Unidos, a las relaciones con otras naciones, etc.

Finalmente, considerando que este método propone la comparación, es necesario establecer que, por tratarse de un estudio de un solo caso, o como lo denominan Goertz & Mahoney, un "*within-case analysis*[9]", la comparación se realiza de forma interna: se compara el caso particular – *Freedom Act* de 2015 – con el instrumento jurídico que modificó, entiéndase el *Patriot Act* y el FISA de 1978.

Marco teórico

A continuación, se presentan las herramientas teóricas a las que recurre el presente trabajo de investigación con el fin de dar cuenta del caso de estudio. En general, este trabajo se basará en el institucionalismo neoliberal y en la interdependencia compleja trazados por Keohane y Nye en la década de 1970, pero desarrollados más adelante por autores como Simmons (2009), Milner & Moravcsik (2009).

El caso de estudio seleccionado necesita un análisis teórico que dé sentido a la relevancia de factores domésticos o internos sobre el sistema internacional, como lo fueron las revelaciones de Edward Snowden. Adicionalmente, necesita comprender el surgimiento de la cooperación a través de instituciones internacionales; estas últimas entendidas de forma amplia, y que engloben sistemas jurídicos, y regímenes internacionales como el de derechos humanos.

[9] Se mantiene en idioma original.

Además, este enfoque teórico nos permite comprender no solo la formación de las instituciones internacionales desde una nueva perspectiva, sino también el cambio o ausencia de él en esas instituciones. Este punto específico permitirá entender, desde la teoría, por qué no existe a nivel internacional un instrumento de regulación sobre privacidad y datos personales. A continuación, se revisarán las bases teóricas con más detalle.

Institucionalismo neoliberal: Keohane y su propuesta de un nuevo paradigma

A mediados de la década de 1970, emergió un nuevo paradigma en la disciplina de relaciones internacionales, fuertemente dominada por el realismo: el institucionalismo neoliberal, consolidado como propuesta teórica por Keohane y Nye. Las ideas articuladas por estos autores, y los que les siguieron los pasos, "están, cada vez más, ganando las batallas empíricas y teóricas en relaciones internacionales, para entender el mundo globalizado" (Milner & Moravcsik, 2009, págs. 3-4).

En primer lugar, el neoliberalismo institucional es una teoría cuyo análisis se plantea desde el nivel sistémico, es decir, considera que el sistema internacional ejerce una influencia determinante sobre los Estados y por ende debe ser ubicado en primer lugar a la hora de explicar los fenómenos. Sin embargo, y a diferencia del realismo que también es una teoría de análisis sistémico, este paradigma considera que los efectos de la anarquía son mitigados tanto por la interdependencia, como por la naturaleza institucionalizada de la política internacional contemporánea (Milner & Moravcsik, 2009).

De acuerdo con Milner & Moravcsik (2009), los cuatro elementos de este paradigma, en contraste con la propuesta realista y neorrealista, son los siguientes: énfasis en actores no estatales, en las formas poder más allá de lo militar, en el rol de la interdependencia y, por último, énfasis en la importancia de la cooperación en la política internacional.

a) Énfasis en actores no estatales, incluyendo las instituciones internacionales

Este paradigma es reconocido, como su nombre lo indica, por su énfasis en las instituciones y regímenes internacionales. Desde una visión más amplia, las instituciones no solo se refieren a organizaciones identificables, con oficinas y personal, sino también a los "principios, normas, reglas y procedimientos decisorios en torno a los cuales las

expectativas de los actores convergen" (Milner & Moravcsik, 2009, págs. 5-6). En la misma línea, Keohane (1998) describe las instituciones como "una categorización o patrón general de actividad, o un arreglo particular de construcción humana, formal o informalmente organizado" (Keohane, 1998, pág. 383). Por eso, es posible afirmar, por ejemplo, que todos los regímenes internacionales son instituciones, esto incluye el derecho internacional y los derechos humanos. También los cuerpos regulatorios dentro de un Estados pueden ser considerados instituciones, porque – de acuerdo con los argumentos de Keohane – es posible identificar en ellos un conjunto de reglas que regula el comportamiento, moldea las expectativas y define roles (Keohane, 1998, pág. 384).

En otras palabras, las organizaciones internacionales son, en efecto, instituciones, pero no todas las instituciones toman la forma de organización. Señalan Milner & Moravcsik (2009) que "para el neoliberalismo institucional, la política internacional está institucionalizada, aunque en diferentes niveles dependiendo de los temas y las regiones" (2009, pág. 6).

Así las cosas, este paradigma sostiene que la relevancia de las instituciones internacionales es indiscutible en la era moderna. Ahora bien, uno de los fenómenos que los distintos teóricos del institucionalismo neoliberal han intentado explicar es el nacimiento y cambio de esas instituciones. En términos generales, se puede decir que los cambios en los regímenes internacionales ocurren cuando se modifica la estructura del tema y/o sus recursos relevantes, por tanto, es la interacción entre poder e interdependencia la que crea el cambio institucional (Milner & Moravcsik, 2009). Sin embargo, se hará énfasis en este aspecto particular más adelante.

b) Énfasis en formas de poder más allá de las fuerzas y amenazas militares

La variedad de las formas de poder en el sistema es un punto distintivo (aunque no exclusivo) de este paradigma. Según explican Milner & Moravcsik (2009): "los recursos de poder para ejercer influencia en el mercado internacional difieren de esos para influir en la no-proliferación nuclear, y de esos para influir en las negociaciones climáticas" (pág. 12). Continúan señalando que, contrario a lo planteado por los realistas, no existe una jerarquía única de recursos de poder, y los Estados varían en sus capacidades de influir sobre los resultados por área de interés.

En relación con el punto anterior, estas capacidades o recursos no provienen únicamente de los Estados. “La idea de la interdependencia compleja sugiere que incluso en situaciones donde todos se benefician de la cooperación, algunos actores tendrán mayor habilidad que otros para influenciar” los resultados de la cooperación (Milner & Moravcsik, 2009, pág. 13).

c) Atención sobre el rol de la interdependencia, además de la anarquía

Los institucionalistas neoliberales describen el sistema internacional como una mezcla de anarquía e interdependencia. A pesar de que parten de un análisis de nivel sistémico, no consideran que la anarquía domine el sistema. Señalan que, incluso en la ausencia de relaciones institucionales, la relación entre Estados tiende a ser marcadamente interdependiente (Milner & Moravcsik, 2009, pág. 15).

Los flujos de bienes, personas, información y capital a través de las fronteras tienen efectos críticos de carácter no solo económico, sino también político. La interdependencia implica un aspecto de gran relevancia en el presente trabajo de investigación: las relaciones transnacionales. Estas relaciones hacen referencia a “múltiples canales que conectan a las sociedades, desde vínculos formales e informales entre diplomáticos, hasta conexiones informales entre élites no gobernantes de diferentes países” (Milner & Moravcsik, 2009, pág. 16).

Ya este paradigma hacía referencia a mediados de los 70 al impacto de la globalización sobre el complejo entramado de relaciones en el sistema internacional, y sus efectos sobre el comportamiento del Estado. Hoy en día, con la aceleración exponencial de la transformación digital, y el desarrollo de avances como la realidad virtual hiper aumentada y el metaverso, estos impactos no solo siguen vigentes, sino que se han profundizado.

d) Foco en la importancia de la cooperación, tanto como la del conflicto en la política internacional.

Este punto es fundamental y uno de los principales planteamientos de Keohane dentro del paradigma. De acuerdo con el autor:

> La cooperación requiere que las acciones de individuos u organizaciones distintos – que no están en armonía preexistente – se pongan en conformidad la una con la

> otra, a través de un proceso de coordinación de política. Esto significa que cuando la cooperación tiene lugar, cada parte cambia su comportamiento en coincidencia con el comportamiento del otro (…) La cooperación es una relación dialéctica donde hay desacuerdo. (Keohane, 1998, págs. 380-381).

Esta posición es interesante, considerando que – contrario a lo que podría pensarse – Keohane no intenta idealizar la cooperación, sino estudiarla. Y para él, si se busca entender la cooperación, también se debe entender la frecuente ausencia, o fracaso, de la misma (Keohane, 1998). Uno de los focos más recurrentes de los académicos dentro de este paradigma es "entender las condiciones bajo las cuales surge la cooperación institucionalizada, o la gobernanza global, con altos niveles de compromiso" (Milner & Moravcsik, 2009, pág. 20).

Compromiso de los Estados con la gobernanza global de Derechos Humanos desde la perspectiva del institucionalismo neoliberal

Utilizando el mismo paradigma, este trabajo de investigación tendrá en cuenta el análisis de Beth Simmons (2009) sobre el nivel de compromiso y cumplimiento de los Estados con las instituciones internacionales orientadas a proteger los derechos humanos, en particular los derechos de las mujeres. Si bien el caso específico no viene al caso, lo que sí vale la pena resaltar en esta sección es el planteamiento teórico que, desde el paradigma del institucionalismo neoliberal, realiza la autora.

En su investigación, Simmons (2009) expone que el origen del compromiso con las instituciones no está en el poder del Estado – como indicarían los realistas – sino más bien un mecanismo complejo que obliga a los Estados a tener en cuenta sus obligaciones dentro de esos acuerdos o marcos.

A diferencia de lo que sucede con otros temas, la aplicación de los acuerdos sobre derechos humanos debe ser descentralizada y recaer en manos de actores no estatales: organizaciones intergubernamentales, grupos activistas transnacionales, y "muy especialmente, *los intereses domésticos que demandan a su gobierno tomar en serio sus compromisos y mecanismos de implementación*[10]" (Milner & Moravcsik, 2009, pág. 13).

[10] Resaltado propio.

La autora señala que, en estos casos, una variedad de actores no estatales ejerce poder sobre los Estados es un contexto de interdependencia compleja (Simmons, 2009).

En los últimos 70 años, los Estados han construido una red extensa de mecanismos e instituciones asociadas a la protección de los derechos humanos, y se han comprometido – a través de este régimen – a cumplir con unos estándares mínimos de protección. La pregunta que eleva Simmons (2009) es si estas instituciones han hecho una diferencia: "¿los gobiernos que se unen a las instituciones derechos humanos protegen a sus ciudadanos mejor que aquellos que no?" (Simmons, 2009, pág. 20). El argumento de la autora es que los gobiernos que se unen a estas instituciones encuentran cada vez más costoso ignorar los principios que estas promueven, más que todo por el impacto a nivel doméstico (Simmons, 2009).

Esto es fundamental para este trabajo de investigación. En el caso que se propone, se busca demostrar que las revelaciones de Edward Snowden generaron un impacto tal sobre el debate público acerca de la privacidad, que presionó al gobierno de Estados Unidos a modificar su legislación vigente en la materia. Más adelante, el desarrollo de los capítulos pretende presentar evidencia suficiente para sostener esta afirmación.

Ahora, es necesario recordar que para 2013 cuando iniciaron las revelaciones, estaba en firme una serie de regulaciones tanto internas como internacionales sobre la privacidad y que buscaban protegerla como un derecho. El más claro ejemplo es la base de todo el régimen de derechos humanos a nivel internacional: la Declaración Universal de Derechos Humanos. En su artículo 12, la Declaración reza:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (Organización de Naciones Unidas, 1948, pág. 203).

Estados Unidos hace parte de la Organización de Naciones Unidas (ONU) y, asimismo, del régimen internacional de protección de derechos humanos desde su origen, a finales de la Segunda Guerra Mundial. Sin embargo, los documentos filtrados por Snowden dejaron en evidencia que el gobierno estadounidense había implementado

prácticas para vigilar la vida y comunicaciones personales de sus ciudadanos, en lo que muchos consideraron una violación de la privacidad por parte de las instituciones gubernamentales.

La entrada de Snowden y de los periodistas y medios de comunicación que este seleccionó para entregarles la información, así como de las empresas tecnológicas en el panorama responde a lo que señala Simmons (2009): la "implementación de los acuerdos [en DD. HH.] está descentralizada y se recarga fuertemente en actores no estatales" (pág.20). En este caso, los intereses domésticos fueron los responsables de poner al gobierno de Estados Unidos a rendir cuentas frente a sus compromisos internacionales de protección de derechos. Este punto se desarrollará más adelante en este trabajo, pero es necesario delinear aquí la utilidad de estos planteamientos teóricos para la comprensión del caso de estudio.

¿Cómo se produce el cambio en las instituciones y regímenes internacionales?

Como se ha mencionado previamente, este trabajo de investigación pretende explicar lo que sucedió con la legislación vigente sobre privacidad en Estados Unidos tras las declaraciones de Edward Snowden. La primera modificación significativa en este sentido fue la adopción del USA Freedom Act de 2015.

A nivel internacional no sucedió igual. Aunque ya existían mecanismos relacionados, no hubo una consolidación de instrumentos internacionales (como un acuerdo, tratado, declaración, etc.) que llevara a garantizar una mayor protección de la privacidad. El régimen internacional de derechos humanos se mantuvo y hoy en día, más allá del artículo 12 de la Declaración Universal de Derechos Humanos, y de algunas consideraciones del Pacto Internacional de Derechos Civiles y Políticos de 1977, no existe un acuerdo específico que vincule a los Estados en esta materia.

Si se considera que tanto el régimen internacional de derechos humanos, como la legislación nacional de Estados Unidos son instituciones – siguiendo la argumentación expuesta sobre la definición de institución en los trabajos de Keohane (1998), Milner & Moravcsik (2009) en el marco teórico del presente texto - es fundamental para esta investigación comprender desde lo teórico cómo y por qué se da el cambio en las instituciones, o, por el contrario, por qué en determinados casos no existe cambio.

Para el institucionalismo neoliberal, “las instituciones cambian en parte por su éxito o fracaso en cumplir las tareas que les fueron delegadas” (Milner & Moravcsik, 2009, pág. 9). Además, lo que los teóricos de este paradigma han señalado, y que es de utilidad para este trabajo de investigación, es que “las instituciones internacionales son lentas en expandirse y adaptarse a nuevas áreas de potencial cooperación por los costos de la negociación y el entramado de intereses de los miembros” (Milner & Moravcsik, 2009, pág. 9).

Como señala Krasner (1982): “los regímenes internacionales deben ser comprendidos como algo más que arreglos momentáneos que cambian a cada modificación de poder o intereses” (pág. 186). Los regímenes son mucho más que acuerdos transitorios. Además, también es fundamental clarificar que hay una diferencia entre principios y normas, por un lado, y reglas y procedimientos, por el otro. Son estas últimas las que definen las características básicas de un régimen internacional, porque

> Puede haber muchas reglas o procedimientos decisorios consistentes con los mismos principios y normas. Los cambios en las reglas y procedimientos decisorios son cambios dentro del régimen y los principios siguen inalterados. (…) los cambios en los principios y normas son cambios del régimen en sí mismo. (Krasner, 1982, págs. 187-188).

En el momento en el cual los principios son abandonados de forma definitiva, es cuando nace un nuevo régimen que reemplaza el anterior, o bien, los regímenes de ese tema desaparecen por completo. Teniendo esto en cuenta, se hace evidente que un cambio de régimen – que es una institución internacional, de acuerdo con los planteamientos del paradigma institucionalista neoliberal – no se presentan tan fácilmente, y constituyen procesos de modificación profunda, no superficial.

Una última observación con respecto al marco teórico del presente trabajo es la justificación de la elección de esta teoría. El institucionalismo neoliberal es una teoría que permite comprender la relevancia de otros actores dentro del sistema internacional, más allá de los Estados. Contempla la importancia de actores no estatales, como las empresas, los individuos, las organizaciones e instituciones internacionales, y permite así dar una mirada más profunda al caso seleccionado.

Adicionalmente, la idea de que las relaciones entre actores del sistema internacional son interdependientes es fundamental, porque contempla los flujos de bienes, personas, información y capital a través de las fronteras como fenómenos relevantes que tienen efectos sobre las decisiones de los Estados y sobre el funcionamiento del sistema.

El presente trabajo busca comprender lo que sucedió en Estados Unidos posterior a las revelaciones de Snowden, en materia de legislación sobre uso y recolección de datos por parte del Estado. Para ello, la teoría debe respaldar el papel que tienen las instituciones, los flujos transnacionales de información y la interdependencia que existe entre esas distintas instancias.

Dicho eso, estos son los planteamientos teóricos que sustentan la argumentación de este trabajo. A continuación, se aborda el desarrollo del caso.

Capítulo 1: ¿qué reveló Edward Snowden? Un análisis del caso a la luz del debate sobre privacidad, vigilancia y uso de datos

Con el fin de iniciar un análisis más detallado del caso de estudio, a continuación, se presenta una descripción breve de lo que contenían los documentos filtrados por Snowden, a través de los medios de comunicación en el verano de 2013.

Las revelaciones

La primera revelación fue el 5 de junio, y consistía de un documento que terminó siendo conocido como la "Orden Verizon" pues era una orden de parte del Tribunal de Vigilancia de Inteligencia Extranjera, o FISC – una institución creada originalmente a través del FISA de 1978 – para que la compañía privada Verizon produjera para la NSA registros telefónicos diarios de las personas, tanto dentro de Estados Unidos como en el extranjero (Fidler, 2015).

Este documento reveló que la NSA, el FBI y el FISC utilizaron las disposiciones del FISA – y de sus respectivas enmiendas, en este caso la sección 215 del *USA Patriot Act* de 2008[11] – para justificar la recolección de datos de las compañías telefónicas como

[11] Enmienda realizada al FISA en 2008, como resultado directo de los ataques de 9-11.

Verizon. Además, el documento hacía explícita la prohibición de revelar el contenido de la orden del Tribunal que autorizada los seguimientos (Fidler, 2015).

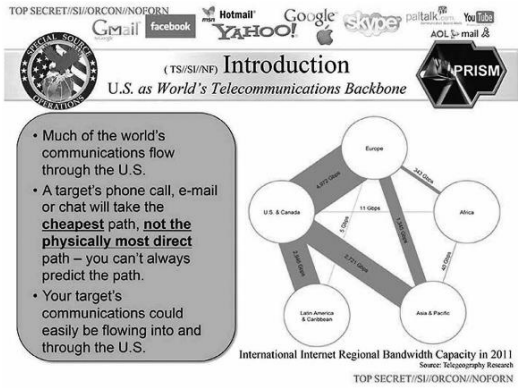
Al día siguiente de la primera revelación, el 6 de junio de 2013, siguió la filtración de dos presentaciones de diapositivas sobre los programas PRISM y UPSTREAM, ambos conducidos por la NSA. La justificación jurídica de estos programas se encontraba también en el FISA, en la sección 702 (Fidler, 2015).

Lo que se dio a conocer en esta segunda revelación fue que el gobierno había sido autorizado para adelantar vigilancia electrónica dentro de Estados Unidos con propósitos de inteligencia, contra ciudadanos extranjeros ubicados fuera de las fronteras del país (Fidler, 2015). En particular, el programa PRISM consistía en el requerimiento por parte de la NSA de que las compañías estadounidenses, como Google y Apple, proveyeran a la institución los datos de las comunicaciones que manejaban de sus objetivos extranjeros. Por su parte, UPSTREAM era la intervención de parte de la NSA de los cables de fibra óptica de propiedad privada que conducían información desde y hacia Estados Unidos para adelantar vigilancia contra objetivos extranjeros (Fidler, 2015).

A continuación, se presenta una de las láminas de la presentación del programa PRISM, revelado por Snowden.

Figura 3

Lámina de introducción al programa PRISM[12]



Fidler, D. P. (2015). *The Snowden Reader*. Bloomington, IN: Indiana University Press. PP-204

[12] Tomado de Fidler (2015). *The Snowden Reader*. Bloomington, IN. Indiana University Press.

Dado que todas las compañías implicadas tenían alcance global, y eran las principales gestoras de datos del mundo, la fuente de información de la NSA a través de estos programas era inagotable y trascendía sin inconveniente todas las fronteras. Estados Unidos aprovechó su posición como columna vertebral de las comunicaciones globales para ejecutar programas de espionaje a gran escala.

Estas revelaciones elevaron el debate sobre las libertades civiles de los ciudadanos, y provocaron la ira de los gobiernos extranjeros, por la violación de la privacidad de sus nacionales por parte de la NSA.

Las reacciones: el ejecutivo, el legislativo y los privados se manifiestan

La filtración de estos documentos creó una tormenta que se extendió por todo Estados Unidos, y después, por el mundo. En 2013 el gobierno de Estados Unidos estaba encabezado por el presidente Barack Obama, quien un par de días después, el 7 de junio de 2013, se pronunció en una rueda de prensa en defensa de la NSA.

En su discurso aseguró que el día que asumió su mandato se comprometió con dos cosas fundamentales: la protección de los ciudadanos estadounidenses, y la defensa de la Constitución, lo cual incluye – según mencionó – el derecho constitucional a la privacidad. Sin embargo, defendió la actuación de la NSA. Los programas revelados, señaló, eran clasificados, pero no secretos pues los comités de inteligencia, el Congreso y otras instituciones los conocían en detalle. Aseguró que el seguimiento telefónico no abordaba el contenido de las llamadas, sino información como duración, números de teléfono y otros (The New York Times, 2013).

El presidente Obama también respaldó los programas en la aprobación previa del Tribunal de Vigilancia de Inteligencia Extranjera, y la existencia de un marco jurídico establecido para la vigilancia, específicamente el FISA y sus respectivas enmiendas. Así mismo, el presidente señaló que los programas son fundamentales porque ayudaban a prevenir ataques terroristas (The New York Times, 2013), una idea que aún era muy relevante en la mente colectiva de la población estadounidense, 12 años después del 9-11. Finalmente, Obama invitó al Congreso a dar el debate entre privacidad y seguridad nacional, y rechazó las filtraciones por considerarlas dañinas en la lucha contra el terrorismo.

De otra parte, hubo reacciones de otros oficiales del gobierno. Fue el caso de Robert S. Litt, de la oficina del Director de Inteligencia Nacional, quien – en la misma línea del Presidente Obama – explicó las actividades de la NSA a la luz de la legislación federal vigente, y defendió los programas PRISM y UPSTREAM alegando su legalidad, efectividad y fidelidad a los valores democráticos de la Constitución de Estados Unidos (Fidler, 2015). Al igual que Obama, Litt señaló que las filtraciones fueron realizadas sin conocer ni entender a fondo los programas de la NSA y, por ende, causaron desinformación y malinterpretación que, en el largo plazo, haría mucho daño a los objetivos de seguridad nacional del Estado (Fidler, 2015).

Uno de los momentos más determinantes de estos primeros meses, fue la declaración del mismo Edward Snowden, revelándose como el origen de las filtraciones y dando pie a que el caso se conociera bajo su nombre. En su discurso desde Moscú señaló que pocos meses antes tenía en su poder la capacidad de obtener y leer las comunicaciones de cada ciudadano estadounidense, en cualquier momento dado, un poder que – a pesar de los intentos de justificación del gobierno – eran ilegales y atentaban no solo contra la Constitución nacional, sino también contra el artículo 12 de la Declaración Universal de Derechos Humanos (Fidler, 2015).

Aseguró que creía firmemente en su obligación de violar las leyes domésticas para prevenir la ocurrencia de crímenes contra la paz y la humanidad y por eso había dejado una cómoda vida de lado, para pasar a ser un exiliado. En una entrevista con Glenn Greenwald y Laura Poitras, de The Guardian, Snowden señaló lo siguiente:

> Cuando se está en una posición de acceso privilegiado, se está expuesto a una gran cantidad de información, más que el empleado promedio dentro de la comunidad de inteligencia. Uno puede reconocer que algunas de estas cosas son en realidad abusos (…) Con el tiempo, la conciencia de la mala conducta se hace más evidente y te sientes obligado a hablar de ello, pero entre más hablas de ellos más frecuentemente te ignoran. Eventualmente entiendes que estas cosas deben ser decididas por el público, y no por un alguien cualquiera contratado por el gobierno (…) Cuando exponer un crimen es tratado

como cometer un crimen, es porque estás siendo gobernado por criminales. (Greenwald & Poitras, 2013, pág. 53).

En sus palabras: “la decisión moral de contarle al público sobre el espionaje que nos afecta a todos ha sido costosa, pero fue lo correcto y no me arrepiento” (Fidler, 2015, pág. 125). Finalizó señalando que el intento de los Estados poderosos de actuar por fuera de la ley representa una amenaza para todos y no se puede permitir (Fidler, 2015).

La misma NSA se defendió. De acuerdo con un artículo de WIRED del 2014, el director de la agencia Richard Ledgett señaló que Snowden era un arrogante por poner las vidas de los ciudadanos en riesgo y que los programas de vigilancia que llevaban a cabo eran en beneficio de la privacidad, y no en su contra (Rowan, 2014). Ledgett fue más allá y expresó que:

> La divulgación descontrolada de las capacidades de la NSA hace que [los objetivos] se alejen de nuestra capacidad de tener conocimiento de lo que están haciendo". Esto beneficiaría no sólo a los terroristas, sino a los traficantes de personas, a los narcotraficantes, a los que intentan construir sistemas de entrega de armas nucleares. Nuestros agentes y aliados corren un mayor riesgo porque no vemos las amenazas que les llegan. Si voy a perseguir a personas que trabajan contra nosotros y nuestros aliados, necesito las capacidades para ir tras ellos (Rowan, 2014, pág. 45)

Así mismo, de parte de la comunidad de inteligencia el Director de Inteligencia Nacional del momento, James R. Clapper, dijo que: “estaba preocupado por el enorme y grave daño que hacen las revelaciones [de Snowden] a nuestras capacidades de inteligencia" (The New York Times, 2013),.

Las reacciones en el Congreso también fueron significativas. Jim Langevin, demócrata del estado de Rhode Island, parte del Comité de Inteligencia de la Cámara de Representantes, dijo que Snowden “ha dañado la seguridad nacional, nuestra capacidad para localizar a los terroristas o a los que tienen intenciones nefastas, y su revelación no ha hecho a Estados Unidos más seguro” (The New York Times, 2013).

En la orilla opuesta, el republicano Jim Sensenbrenner, uno de los coautores del Patriot Act del 2008 y que trabajó con la administración de George W. Bush tras los ataques del 9-11, dijo que "la comunidad de inteligencia ha dado mal uso a sus poderes al recolectar los registros telefónicos de todos los ciudadanos, por lo cual es tiempo de poner los programas de meta data fuera del negocio" (The Guardian, 2013).

Un mes después de las revelaciones iniciales, en julio, se presentó en la Cámara de Representantes una propuesta para eliminar los programas de vigilancia telefónica por parte de los representantes Justin Amash y John Conyers. De acuerdo con Fidler (2015): "este fue el esfuerzo legislativo de más alto perfil para prevenir que el gobierno de Estados Unidos recolectara meta data telefónica de los estadounidenses" (pág. 115). El proyecto no pasó, pero con una votación 217-205 se hizo evidente la polarización de los congresistas en torno a la vigilancia gubernamental. En esa misma línea, el medio Político señaló en una nota de agosto de 2013 que:

> Ya se han presentado más de una docena de proyectos de ley para poner fin al programa de recopilación masiva de registros telefónicos de la NSA y para revisar el Tribunal de Vigilancia de Inteligencia Extranjera, que ha reinterpretado la Cuarta Enmienda en secreto, creando un cuerpo de leyes de privacidad que el público nunca ha leído. Se han presentado media docena de nuevas demandas sobre privacidad contra la NSA. El Pentágono está siendo sometido a una auditoría de secreto sin precedentes. Funcionarios estadounidenses han sido sorprendidos engañando o mintiendo al Congreso y la lista sigue (Timm, 2013, pág. 104).

La postura de defensa de Snowden, tan criticada por la comunidad de inteligencia y por el gobierno, era en cambio compartida por la opinión pública. Esto lo demuestra una encuesta de Quinnipac publicada a finales de julio de 2013 y revelada en medios de comunicación en Estados Unidos. Los resultados indicaron que el 55% de los ciudadanos estadounidenses encuestados veían a Snowden más como un "denunciante[13]" que como

[13] Denunciante como traducción del término *whistleblower*, en inglés.

un traidor, resultado que se repetía tras una encuesta similar justo después de las revelaciones (Kopan, 2013).

La posición del público estadounidense continuó favoreciendo a Snowden. De hecho, en octubre de 2013 se registraron marchas en contra de los programas de vigilancia de la NSA, como narra un artículo de prensa de CNBC del domingo 27 de octubre:

> Los manifestantes marcharon el sábado en el Capitolio de Washington para protestar contra los programas de vigilancia en línea del gobierno de Estados Unidos, cuyo vasto alcance fue revelado este año por el excontratista Edward Snowden. La gente llevaba pancartas en las que se leía: "Alto al espionaje masivo", "Gracias, Edward Snowden" y "Desenchufa al Gran Hermano", mientras se reunían al pie del Capitolio para manifestarse contra la de la NSA. (CNBC, 2013, pág. 32).

Esta manifestación, como otras posteriores, fue organizada por una coalición llamada “Dejen de vigilarnos”[14] que reunía alrededor de 100 colectivos, compañías y organizaciones activistas incluyendo a la Unión Americana de Libertades Civiles (ACLU), el grupo de privacidad Electronic Frontier Foundation, Occupy Wall Street NYC y el Partido Libertario (CNBC, 2013).

Como señala el mismo medio, CNBC, “los grupos han instado al Congreso a reformar el marco legal que respalda la recopilación de datos por parte de la NSA, desde que Snowden reveló información clasificada sobre los programas de inteligencia” (CNBC, 2013).

Los gobiernos extranjeros también se pronunciaron sobre las revelaciones. En particular, el gobierno del Reino Unido que en ese momento estaba presidido por el Primer Ministro David Cameron. En una posición de rechazo hacia las actuaciones de Snowden, Cameron señaló que “las filtraciones han causado un profundo daño a la seguridad nacional” y pidió que se investigara a The Guardian por su participación en las revelaciones (The Guardian, 2013)

[14] *Stop Watching Us* en inglés.

En la misma línea, Liam Fox, miembro del Parlamento británico y antiguo secretario de defensa de ese país se pronunció en la Cámara de los Comunes: "¿Podemos tener una evaluación completa y transparente sobre si la implicación de The Guardian en el caso Snowden ha dañado la seguridad nacional? (...) es extraño que The Guardian afirme que dejar los secretos de Gran Bretaña y el personal de seguridad más vulnerables es abrir un debate sobre la responsabilidad de los servicios de seguridad" (The Guardian, 2013). El Primer Ministro Cameron invitó a los comités existentes en el Parlamento a decidir si era pertinente revisar más a fondo la responsabilidad del medio en todo el asunto.

El mismo mes de las revelaciones, junio de 2013, una encuesta de YouGov contratada por el medio Sunday Times en Reino Unido, arrojó que la mayoría del pueblo británico estaba de acuerdo con las filtraciones y consideran que Snowden no debería ser procesado por la justicia por sus actuaciones (YouGov PLC, 2013). Según la encuesta, el 56% de los británicos dijo que Snowden tenía el derecho de revelar a los medios cómo el gobierno de Estados Unidos monitoreaba correos y llamadas, contra solo el 27% que opinó lo contrario. Además, 52% de los encuestados respondió que Snowden no debería tener cargos en su contra (YouGov PLC, 2013).

El rechazo del gobierno británico fue tal, que incluso prohibió a los aeropuertos recibir a Snowden en territorio nacional, pues esto sería dañino para el bien colectivo (The Guardian, 2013). Además, el Primer Ministro Cameron intentó restar importancia al impacto de las revelaciones, señalando lo siguiente: "Creo que la reacción del público, tal y como yo la juzgo, no ha sido de horror, sino más bien de *"las agencias de inteligencia realizan un trabajo de inteligencia: bien*", e instó a los medios como The Guardian y The Washington Post, a "pensar bien antes de actuar porque estamos en riesgo de volvernos más inseguros como país como resultado de esto" (Solon, 2014).

Por último, vale la pena destacar en esta sección la reacción del sector privado. Según señala Fidler (2015):

> Las empresas tecnológicas estadounidenses ya se enfrentaban a problemas en los mercados mundiales debido a las revelaciones de Snowden sobre la focalización de las

> comunicaciones extranjeras a través de la vigilancia de la NSA y el espionaje de Estados Unidos a gobiernos, líderes y empresas extranjeras (Fidler, 2015, pág. 145).

En este contexto, las compañías tuvieron que tomar acciones de cara al público. Ejemplo de ello es la declaración de Marissa Mayer, CEO Yahoo!, en noviembre de 2013. En ella, Yahoo! toma postura frente a las revelaciones de Snowden y anuncia nuevas medidas de seguridad en sus plataformas para proteger la privacidad de los usuarios (Ver Anexo 1) (Mayer, 2013).

A finales de 2013, las compañías del sector se unieron en una postura pública para promover la reforma legislativa, abogando por mayor protección de los usuarios. Además, enviaron una carta abierta al Presidente Obama, pidiendo más control a la vigilancia gubernamental (Ver Anexo 2) (CBC News, 2013). Las compañías en cuestión fueron AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter y Yahoo! (Fidler, 2015).

Capítulo 2: *USA Freedom Act* de 2015, la respuesta de Estados Unidos en la era post-Snowden

Este capítulo busca explicar el *USA Freedom Act* de 2015, o la Ley de Libertad Estadounidense, como un producto de las revelaciones de Snowden. Esta ley federal fue la respuesta del gobierno de Estados Unidos frente a las recias críticas que recibió, tanto a nivel doméstico como internacional, tras conocerse el alcance de sus programas de vigilancia. Es la primera consecuencia legislativa identificable del impacto de las revelaciones.

Primero, se traza el antecedente principal del *Freedom Act* y es la Ley de Vigilancia de Inteligencia Extranjera o FISA, por sus siglas en inglés. Esta fue la ley que el *Freedom Act* modificó, y fue la que dio bases legales a las actividades de vigilancia del gobierno de Estados Unidos. Luego se hace un breve resumen de las revelaciones de Snowden, explicando los tres documentos principales: el documento Orden Verizon, y las presentaciones de los programas PRISM y USPTREAM.

Más adelante se enumeran algunas de las reacciones frente a las revelaciones, y finalmente, se expone la Ley de Libertad Estadounidense de 2015, y sus principales

disposiciones con respecto a la recolección de datos, y vigilancia por parte del Estado con fines de seguridad nacional.

Generalidades

Como se ha venido estableciendo, el caso Snowden uno de los momentos más emblemáticos de la historia reciente en materia de libertades individuales, no solo en Estados Unidos sino a nivel global. Esto no significa que otros casos no hayan dejado antes en evidencia el alcance y las posibles extralimitaciones del Estado en materia de vigilancia, pero este caso en particular llama mucho la atención porque se dio en un escenario de avance tecnológico sin precedentes, con niveles de interconexión e interceptación de los datos en el ciberespacio que llevan las capacidades del Estado en materia de vigilancia a otro nivel.

> Eran finales de mayo de 2013 cuando un profesional estadounidense en computación atravesaba la puerta del Aeropuerto Internacional de Hong Kong (…) Estaba a punto de cometer el mayor acto de denuncia en la historia de las instituciones modernas de inteligencia, que sería nombrado en honor a él: las revelaciones Snowden. (Pohle & Van Audenhove, 2017, pág. 1).

De hecho, parte del problema era que los documentos filtrados revelaban que la vigilancia trascendía las fronteras nacionales de Estados Unidos, y se extendía a otros Estados. Por eso, según la observación de Kampmark (2014), las revelaciones de Snowden sugerían la globalización del Estado vigilante. A raíz de esto, y como señala Fidler (2015), se transformó la política exterior de Estados Unidos sobre el ciberespacio: “las revelaciones arrasaron con la perspectiva de la libertad en Internet y forzaron al gobierno a defenderse de lo que las filtraciones desataron, en casa y en el exterior” (pág. 56).

Foreign Intelligence Surveillance Act 15(FISA), el antecedente de las actividades de vigilancia en Estados Unidos

Tras las revelaciones de Snowden, y casi de la noche a la mañana, los ciudadanos estadounidenses conocieron una serie de programas de inteligencia del gobierno que recolectaban una cantidad muy significativa de datos personales. Si bien la vigilancia no era algo nuevo, el alcance de estos programas causó sorpresa e indignación entre la ciudadanía, que sentía vulnerada y que equiparó estas actividades con el trato que se daba a los "terroristas", pero en contra de ciudadanos comunes. Así lo demostraron las encuestas de opinión y las manifestaciones de los meses posteriores a las revelaciones, documentadas por artículos de prensa nacional (CNBC, 2013) (Kopan, 2013).

Como expone un artículo de CNBC, los ciudadanos de todas las orillas políticas buscaban un cambio en las actividades de vigilancia del Estado. Michael Greene, un ciudadano que habló con CNBC en una de las marchas en Washington DC señaló que: "Me considero un conservador y ningún conservador quiere que su gobierno recopile información sobre ellos y la almacene y utilice" (CNBC, 2013).

Así mismo, Jennifer Wynee dijo al mismo medio que: "En los últimos meses, hemos aprendido mucho sobre los abusos de la privacidad que están ocurriendo y la completa falta de supervisión y la vigilancia masiva en cada detalle de nuestras vidas. Tenemos que decirle al Congreso que tiene que actuar" (CNBC, 2013).

En términos legales, la recolección de datos por parte de la NSA estaba siendo auspiciada por el *Foreign Intelligence Surveillance Act* de 1978 (Ley de Vigilancia de Inteligencia Extranjera), o FISA, una ley federal de Estados Unidos que fue acogida para establecer los procedimientos de vigilancia y compilación de datos con fines de seguridad nacional e inteligencia extranjera.

Hasta ese momento esta ley había jugado un papel fundamental en la respuesta al terrorismo y en la defensa de la seguridad nacional, especialmente después de los ataques de 11 de septiembre de 2001 (Kerr, 2008). El FISA daba vía libre al Estado para recolectar

[15] En algunos momentos del texto se mantiene el nombre en su idioma original.

y almacenar robustas bases de datos con información de meta data basada en la actividad telefónica de los ciudadanos (Berman, 2016).

Casi desde su aprobación, el FISA enfrentó críticas y se vio envuelto en controversias y reformas. La pregunta de fondo fue siempre la misma, ¿esta ley logra el balance adecuado entre seguridad nacional y privacidad? (Kerr, 2008), una pregunta que no ha dejado de estar justo en el centro del debate.

Ley de Libertad Estadounidense o *USA Freedom Act*: la respuesta de Estados Unidos

El 28 de abril de 2015, el proyecto de ley de lo que sería la Ley de Libertad Estadounidense fue presentada en el Congreso, en la Cámara de Representantes. En la presentación del texto, en la sección de "Antecedentes y necesidad de la ley" se menciona directamente el caso Snowden y se desglosa el marco legal que permitió la vigilancia de la NSA, el FISA de 1978 y sus enmiendas correspondientes.

Según el texto, la nueva ley busca prohibir la recolección masiva de datos, crea un nuevo programa de recolección selectiva de metadatos telefónicos, expande las capacidades del Congreso para vigilar estas acciones y busca proveer más transparencia y mayor protección de la privacidad y las libertades civiles de los ciudadanos (United States 114th Congress, 2015).

El 13 de mayo el proyecto fue aprobado en la Cámara con votación 338-88, y el 2 de junio siguiente pasó con votación 67-32 en el Senado. El mismo día fue sancionada por el presidente y se convirtió en la Ley Federal Nº114-23 de los Estados Unidos (Ver Anexo 3). Sin embargo, esto no terminó con el debate: algunos congresistas celebraron la nueva legislación, afirmando que era un avance sin precedentes en materia de control de las acciones de vigilancia, mientras que otros se opusieron, considerando que no era suficiente.

El senador Rand Paul, republicano del Estado de Kentucky, se expresó de esta forma en favor de la Ley de Libertad:

> Llega un momento en la historia de las naciones, en el cual el miedo y la complacencia le permiten al poder acumularse, en detrimento de la libertad y la

> privacidad. Ese momento es ahora, y no dejaré que la Ley Patriótica (Patriot Act), la más antipatriótica de las leyes, continúe sin oposición (The New York Times, 2015).

En la misma línea, la senadora Dianne Feinstein, demócrata de California señaló lo siguiente: "Para los que quieren una reforma, y quieren prevenir que el Estado mantenga los datos, la Ley de Libertad es la única forma de hacerlo" (The New York Times, 2015). Por el contrario, Barbara Mikulski, senadora demócrata de Maryland, dijo que: "no podemos dejar que este país se oscurezca en términos de su habilidad para hacer su deber de defender a los Estados Unidos de América" (The New York Times, 2015).

El senador Mike Lee, republicano del estado de Utah, señaló que comparte posiciones con el senador Paul sobre la recolección masiva de metadatos, pues "ambos consideramos que está mal que el gobierno recolecte registros telefónicos de todos los ciudadanos" (The New York Times, 2015).

Algunos políticos fuera del Congreso se pronunciaron sobre el debate. Es el caso del gobernador Chris Christie, republicano de New Jersey, quien señaló que: "la obligación principal del gobierno de Estados Unidos es proteger la vida del pueblo estadounidense, y eso lo podemos hacer de una forma inteligente, costo-efectiva y al mismo tiempo protegiendo las libertades civiles, pero ¿saben? No se puede disfrutar de las libertades civiles si se está en un ataúd" (The New York Times, 2015).

De nuevo, citando al senador Paul, una de las mayores discusiones era sobre a quién iban dirigidas esas medidas. En sus palabras: "No estamos recolectando información de espías, ni la información de los terroristas, estamos recolectando información de todos los ciudadanos estadounidenses, todo el tiempo, es por esto por lo que peleamos una revolución" (The New York Times, 2015).

Por su parte, y en una posición más conciliadora, el senador James Lankford, republicano de Oklahoma, señaló que la seguridad y la privacidad no son mutuamente excluyentes, y que ambas pueden conseguirse a través de una vigilancia responsable y el respeto por los ciudadanos que cumplen la ley (The New York Times, 2015).

Mitch McConnell, senador republicano de Kentucky fue el mayor opositor de esta ley en el Congreso. Desde el principio mantuvo que esta significaría una reducción peligrosa de la seguridad nacional y que aprobar la ley sería un ataque directo que quitaría

herramientas valiosas a aquellos que día a día defienden la nación (United States 114th Congress, 2015), (The New York Times, 2015).

La discusión en el congreso fue liderada principalmente por el Partido Demócrata y por una nueva generación de republicanos. Según señala el medio The New York Times, (2015), aunque las amenazas de seguridad se multiplicaron desde los ataques del 9/11, las preocupaciones en torno a la privacidad, alimentadas por las revelaciones sobre las brechas de seguridad en las compañías privadas, y las extralimitaciones del gobierno, fueron las que hicieron su efecto sobre la opinión pública.

En todo caso, la Ley de Libertad Estadounidense entró en vigencia el 6 de junio de 2015, dos años después de las revelaciones. En resumen, esta ley prohíbe la recolección masiva de los registros privados de los ciudadanos estadounidenses, bajo la sección 215 del *Patriot Act* – la enmienda que fue utilizada como justificación por el FISC para el programa PRISM. La ley contempla modificaciones significativas a las autoridades de la Comunidad de Inteligencia que el gobierno utilizó durante años como justificación de sus acciones de vigilancia telefónica y en internet a través de recolección masiva de meta data (United States 114th Congress, 2015).

De acuerdo con el acto legislativo, esta ley busca:

> Reformar las facultades del Gobierno Federal para exigir la presentación de determinados registros comerciales, llevar a cabo vigilancia electrónica, utilizar registros de llamadas y dispositivos de seguimiento, y utilizar otras formas de recopilación de información con fines de inteligencia extranjera, antiterroristas y criminales, y para otros fines. (United States 114th Congress, 2015).

Esta ley exige al gobierno limitar todo lo posible la recolección de información relacionada con un proveedor específico, o una región, ciudad o territorialidad definida (United States 114th Congress, 2015). Sin embargo, esto no significa que la vigilancia como tal esté prohibida, sino más bien que la Comunidad de Inteligencia de Estados Unidos puede recolectar datos, pero de una forma más focalizada y con previa autorización judicial, para reemplazar la vigilancia masiva e indiscriminada.

Además, la nueva ley incluye una serie de requerimientos de reporte a las autoridades del FISA, orientados a aumentar la transparencia sobre las acciones de vigilancia (United States 114th Congress, 2015). También solicita la creación de un panel de expertos en privacidad, libertades civiles y tecnología para ofrecer consejo y consultoría al FISC (The Transatlantic Digital Dialogue German Marshall Fund of the United States, 2015), y abre la posibilidad de instancias de apelación para las decisiones del FISC (United States 114th Congress, 2015).

Capítulo 3: Análisis del caso a la luz de la interdependencia compleja y el institucionalismo neoliberal

La aprobación y entrada en vigor de la Ley de Libertad Estadounidense en junio de 2015 es, como se ha visto, una consecuencia directa de la situación interna que desató Snowden con las filtraciones de documentos clasificados de inteligencia.

Recordando los planteamientos del institucionalismo neoliberal, expuesto en el marco teórico del presente trabajo de investigación, se observa que en este caso fue la presión de actores no estatales, como las empresas privadas que dieron origen al primer texto de la Ley de Libertad Estadounidense, y la misma opinión pública, la que obligó al Estado a tomar acciones de reforma y modificar su legislación para ajustarse no solo a la Constitución, sino a los compromisos internacionales derivados del régimen internacional de Derechos Humanos, mencionado por el mismo Snowden.

Además, se observa que – siguiendo el análisis desde el mismo paradigma – las denominadas relaciones transnacionales juegan en este caso un papel determinante. Los flujos de información que se movían de manera masiva a través de las redes de compañías globales como Google o Facebook terminaron convirtiéndose en un factor de poder para Estados Unidos, y para las mismas empresas, a la hora de adelantar sus programas de vigilancia más allá de sus fronteras. Como demostraron los documentos filtrados, la Comunidad de Inteligencia de Estados Unidos demostró que fue gracias al poder que les confería su posición como punto de convergencia de los flujos globales de información que pudieron adelantar programas de vigilancia del alcance observado. Esos mismos

flujos de información fueron los que garantizaron que a nivel global se conocieran las implicaciones de las revelaciones. La globalización de los flujos de datos es un punto que está en el corazón del caso seleccionado.

Volviendo a las instituciones, uno de los papeles de estas instituciones, si seguimos el análisis de Keohane (1998), es el de moldear las expectativas. Las reacciones que se presentaron por parte de actores no estatales tras las revelaciones dejan ver que parte del impacto inicial de este caso se dio por la incongruencia entre las expectativas derivadas de la institución, y la realidad de las acciones del Estado reveladas por Snowden.

Otro punto donde se ven reflejados los planteamientos de este paradigma es en los recursos de poder para influenciar en la cooperación. Parece interesante que, derivado de su enorme poder económico, las empresas privadas de tecnología pudieran influir de manera tan determinante en el debate y en el resultado de este caso: la aprobación de la Ley de Libertad Estadounidense en 2015. En este caso, el recurso económico les dio poder a las compañías para influenciar el resultado.

Así mismo, el acceso a los masivos flujos de información le dio poder a Estados Unidos en la arena internacional, al facilitar sus intentos de garantizar su seguridad nacional a través de la vigilancia que trascendía fronteras. Los otros Estados quedaron, en algunos casos, en posición relativa de desventaja al no tener ese mismo acceso, que en este caso se puede interpretar cono un factor relativo de poder en el sistema. La información misma se traduce en poder en un sistema internacional hiperglobalizado como el que vemos actualmente.

Otro aspecto que en este punto es crucial destacar es el rol de la interdependencia, elaborado por los teóricos del institucionalismo neoliberal. Como bien se planteó antes en este trabajo de investigación, los académicos de este paradigma consideran que, si bien la anarquía es esencial en el sistema internacional, también es necesario reconocer el alto nivel de interdependencia y el grado avanzado de institucionalización del sistema.

Está claro que Estados Unidos logró traspasar la línea de protección de la privacidad de los ciudadanos, consignada como un derecho universal y además incluida en la Constitución nacional, a través de programas masivos de espionaje. Si consideramos

la naturaleza anárquica del sistema, es comprensible que ninguna entidad supranacional pudiese impedir estas actuaciones. Sin embargo, lo que este caso nos demuestra es que hay otros factores en juego que modificaron el curso de acción de Estados Unidos, tanto a nivel doméstico como internacional.

Las relaciones transnacionales, que son esos canales o vasos comunicantes que conectan sociedades entre sí, fueron fundamentales en este caso. Se vio reflejado tanto en los flujos de información – que aceleraron la masificación del caso Snowden y lo llevaron a cada rincón del planeta, convirtiéndolo en un fenómeno global, pero que a su vez se convirtieron en un factor de poder en la dimensión internacional – como en la participación y relevancia de actores no estatales.

Si Estados Unidos no tuviese influencia de esas relaciones y flujos transnacionales, probablemente podría haber continuado con sus actividades justificado en la búsqueda de la seguridad nacional, aunque ese argumento tuviese de por sí sus propios problemas y detractores – esa es otra discusión. Es la interdependencia con otros actores, tanto estatales como no estatales, lo que determinó el resultado de este caso particular. Como señalan los institucionalistas neoliberales, las relaciones transnacionales tienen efectos sobre el comportamiento del Estado (Milner & Moravcsik, 2009) y ese fenómeno se ha visto profundizado a niveles que seguramente los teóricos iniciales de este paradigma ni siquiera imaginaron.

Finalmente, vale la pena sumar un último análisis desde este paradigma. En el marco teórico se referenció el estudio de Beth Simmons (2009) sobre el nivel de compromiso y cumplimiento de los Estados con los regímenes internacionales de derechos humanos. La autora mencionada plantea que el nivel de compromiso depende de un mecanismo completo que obliga a los Estados a considerar sus obligaciones dentro de estos acuerdos o marcos.

Este caso es un ejemplo de esta afirmación. Pues el papel de los actores no estatales en presionar al gobierno de Estados Unidos en el cumplimiento de sus compromisos internacionales con la protección de derechos humanos fue clave. Como señaló la autora, “los intereses domésticos demandan a su gobierno tomar en serio sus compromisos y mecanismos de implementación” (Simmons, 2009, pág. 13). Esa

influencia es posible únicamente partiendo del supuesto de la relación de interdependencia que existe entre los diferentes actores.

Tanto Snowden, como la opinión pública, como las empresas privadas y los otros Estados presionaron, de forma conjunta e interrelacionada – a Estados Unidos para que actuara en conformidad con el respeto por el derecho de sus ciudadanos a la privacidad y limitara sus programas de recolección de datos, dando origen a la Ley de Libertad Estadounidense.

Otra consideración es el asunto del cambio. Desde el paradigma del institucionalismo neoliberal, con autores como Milner y Moravcsik (2009), se explica que las instituciones internacionales son lentas en expandirse y adaptarse a nuevas áreas de cooperación. Esto parece reflejarse en el caso de estudio porque, a pesar de que hay una serie de instrumentos y regulaciones sobre privacidad desde hace décadas, esas disposiciones están lejos de garantizar aplicabilidad para las condiciones de hoy. Hace 70 años la privacidad era más fácil de definir, pues las barreras entre lo privado y lo público estaban mejor determinadas. Hoy en día, las barreas son difusas, y la vida privada está sometida de forma constante a la esfera pública por la irrupción de Internet, las redes sociales y más adelante, los escenarios de realidad virtual y el metaverso.

En suma, la regulación sobre derecho a la privacidad ha tardado en ajustarse. Incluso, en el caso específico de Estados Unidos, ya desde la década de 1980 – o incluso antes – se discutía sobre la necesidad de ajustar la regulación interna sobre temas de vigilancia, en ese momento enarbolada principalmente por el FISA. Si en ese momento ya existía la discusión, se entiende que, en la realidad actual de transformación acelerada, siga siendo pertinente y necesario ese debate.

Conclusiones

El presente trabajo de investigación se presentó con el fin de determinar cuál había sido el curso de eventos, fenómenos y procesos que llevaron a Estados Unidos a adoptar la Ley de Libertad Estadounidense en 2015, exactamente 2 años después de las revelaciones de Edward Snowden sobre los programas de vigilancia masivo del gobierno y sus instituciones de inteligencia.

La pregunta de investigación que se planteó como guía fue la siguiente: **¿Cómo se explica la modificación de la legislación sobre privacidad y protección de datos en Estados Unidos, específicamente a través del Freedom Act de 2015, en el contexto posterior a las revelaciones de Edward Snowden?**

Con el desarrollo del presente trabajo, y dando respuesta a esa pregunta, se encontró lo siguiente: la adopción de la Ley de Libertad Estadounidense de 2015 fue una consecuencia directa de varios fenómenos que se desataron tras las revelaciones de Edward Snowden. Con las filtraciones, que iniciaron en 2013, se creó un ambiente interno e internacional propicio para la reforma legislativa: una opinión pública que presionaba por la reforma, un sector privado que se volcó en contra de la institucionalidad de inteligencia para sumarse a la ola reformista, unos gobiernos extranjeros que tuvieron mucho que opinar sobre las revelaciones, y una presión por parte de los medios de comunicación para limitar el alcance de la vigilancia gubernamental.

Esto no quiere decir que todos los actores estuvieran a favor de la reforma, de hecho, se generó un amplio debate donde los gobiernos, especialmente el de Estados Unidos y su comunidad de inteligencia, se defendieron frente a las críticas y argumentaron en favor de la vigilancia con fines de seguridad, antiterrorismo y otros. En contraposición estuvo la opinión pública, que mayoritariamente se puso del lado de Snowden, especialmente durante los meses posteriores a las revelaciones, los medios de comunicación, y algunas figuras relevantes en el escenario político, como congresistas y exfuncionarios.

A pesar del debate, finalmente el gobierno y el Congreso terminaron favoreciendo una reforma a la legislación sobre vigilancia estatal, que se consolidó en la Ley de Libertad Estadounidense.

Ahora bien, este trabajó se enmarcó en una posición de análisis desde el institucionalismo neoliberal, buscando dar sentido a las complejas relaciones entre actores no estatales (empresas, individuos, etc.) y estatales para dar lugar a un proceso de institucionalización o a un resultado tangible: la Ley de Libertad Estadounidense.

Desde ese análisis es posible concluir que la combinación específica de factores fue la que dio origen al resultado observado: desde el punto de hiperglobalización del sistema, hasta los antecedentes domésticos de la discusión sobre seguridad nacional y privacidad.

Además, es posible concluir que una teoría como esta, que se desarrolló en la década de 1970, sigue siendo muy vigente y demostró poder explicar el caso de estudio, en un contexto histórico muy distinto al que existía cuando el paradigma se consolidó dentro de la disciplina.

Parte de la preocupación que dio origen al trabajo de investigación aquí presentado es la sensación de vulnerabilidad derivada de la creciente penetración de la tecnología. En el mundo actual parece inevitable escapar de la vigilancia por parte de gobiernos y grandes corporaciones. Por ello parece necesario, y es lo que el caso de este estudio muestra, ajustar las regulaciones de tal forma que respondan a la situación actual de los avances tecnológicos y los masivos flujos de información.

Actualmente existen regulaciones e instrumentos en pie para asegurar la protección de los derechos humanos, específicamente de la privacidad, tanto a nivel estatal como a nivel internacional. Sin embargo, las condiciones del sistema internacional anárquico muchas veces hacen posible que los actores cometan acciones que atenten contra esas regulaciones o regímenes.

A pesar de ello, lo que este trabajo de investigación logró demostrar es que – a pesar del efecto de la anarquía – las relaciones transnacionales, la participación de actores no estatales y la interdependencia que existe entre todos ellos es también determinante a la hora de que se produzca un resultado en el sistema.

Otro punto para concluir es que la discusión o tensión entre seguridad nacional y derechos individuales seguirá presente. En un mundo con crecientes amenazas a la seguridad que provienen de fuentes diversas y, muchas veces, difusas, la garantía de la seguridad nacional por parte de los Estados es cada vez más compleja. Esto significa que, si bien se puede avanzar en el fortalecimiento de los instrumentos que protegen los derechos de los ciudadanos, el cambio en el entorno está siendo tan acelerado que es posible que nunca sea suficiente.

Es por esa razón que, de cara a investigaciones futuras, valdría la pena seguir el camino que otros académicos de la disciplina y del derecho han trazado ya: ¿es posible avanzar hacia un régimen internacional de protección de la privacidad? Antes, cuando la Declaración Universal de Derechos Humanos fue adoptada por la comunidad internacional, ya se contemplaba este derecho, pero las implicaciones que tiene hoy en día son diametralmente diferentes, empezando solamente por la irrupción del Internet.

Finalmente, es necesario destacar que el caso Snowden es solo una manifestación más de las complejas interacciones que existen en el sistema y que tenderán a profundizarse a medida que la tecnología y las transformaciones dadas por avances en la dilución de fronteras entre la realidad material y la virtual se consoliden.

Referencias

Bass, L. (2019). The concealed cost of convenience: protecting personal data privacy in he age of Alexa. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 261-324.

Berman, E. (2016). The two faces of the forign intelligence surveillance court. *Indiana Law Journal*, 1191-1250.

Biscontini, T. (2021). *Surveillance Capitalism.* Salem Press Encyclopedia.

Brenner, S., & Clarke, L. (2007). Should commercial misuse of private data be a crime? En H. Chen, T. Raghu, R. Ramesh, A. Vinze, & D. Zeng, *National Seciruty* (págs. 3-24). Amsterdam: Elsevier.

CBC News. (9 de Dec de 2013). *NSA spying: Facebook, Google, Twitter demand controls*. Obtenido de CBC: https://www.cbc.ca/news/world/nsa-spying-facebook-google-twitter-demand-controls-1.2456259

CNBC. (27 de Oct de 2013). *Protesters march in Washington against NSA spying*. Obtenido de CNBC: https://www.cnbc.com/amp/2013/10/27/protesters-march-in-washington-against-nsa-spying.html

Coyne, H. (2019). The Untold Story of Edward Snowden's Impact on the GDPR. *The Cyber Defence Review*, 65-80.

Drezner, D. (2011). Weighing the Scales: The Internet's Effects on State-Society Relations. En R. Subramanian, & E. Katz, *The Global Flow of Information: Legal, Social and Cultural Perspectives* (págs. 121-138). New York: New York University Press.

Fidler, D. P. (2015). *The Snowden Reader.* Bloomington, IN: Indiana University Press.

Gellman, B. (2020). *Dark mirror: Edward Snowden and the american surveillance state.* New York: Penguin Press.

Gellman, B. (11 de Mayo de 2020). Secrets, Sirveillance and Snowden. *The Washington Post Magazine*. Obtenido de https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/

Giacomello, G. (2014). *Security in cyberspace: targetting nations, infrastructures, individuals.* New York: Bloomsbury.

Goertz, G., & Mahoney, J. (2012). *A tale of two cultures. Cualitative and Quiantitative Research in Social Sciences.* Princeton: Princeton University Press.

Greenwald, G. (2017). The Surveillance State. En S. Khorana, J. Henrichsen, E. Bell, & T. Owen, *Journalism after Snowden: The future of the free press in the surveillance state* (págs. 34-52). New York: Columbia University Press.

Greenwald, G., & Poitras, L. (6 de Jun de 2013). *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'*. Obtenido de The Guardian: https://www.youtube.com/watch?v=0hLjuVyIIrs

Hagan, M. (2022). *Edward Snowden.* Salem Press Biographical Encyclopedia.

Heisenberg, D. (2005). *Negotiating Privacy : The European Union, the United States, and Personal Data Protection.* London: Lynne Rienner Publishers.

Howard, P. (2010). Triangulating Debates Within the Field: Teaching International Relations Research Methodology. *International Studies Perspectives*, 393-408.

Kampmark, B. (2014). Restraining the Surveillance State: A Global Right to Privacy. *Journal of Global Faultlines*, 1-16.

Keohane, R. (1998). International institutions: two approaches. *International Studies Quarterly*, 379-396.

Kerr, O. (2008). Updating the Foreing Intelligence Surveillance Act. *The Uniersity of Chicago Law Review*, 225-243.

Khorana, S., Henrichsen, J., Bell, E., & Owen, T. (2017). *Journalism After Snowden : The Future of the Free Press in the Surveillance State.* New York: Columbia University Press.

Klotz, A. (2008). Case Selection. En A. Klotz, & D. Prakash, *Qualitative Research Method in International Relations* (págs. 43-58). New York: Palgrave Macmillan.

Kopan, T. (1 de Aug de 2013). *Poll: Snowden still a whistleblower*. Obtenido de Politico: https://www.politico.com/story/2013/08/edward-snowden-nsa-leak-poll-095054

Krasner, S. (1982). Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, 185-205.

Mayer, M. (18 de Nov de 2013). *Our Commitment to Protecting Your Information*. Obtenido de Yahoo!: https://yahoo.tumblr.com/post/67373852814/our-commitment-to-protecting-your-information

Milner, H., & Moravcsik, A. (2009). *Power, Interdependence and Nonstate actors in Wrold Politics.* Princeton: Princeton University Press.

Organización de Naciones Unidas. (10 de Diciembre de 1948). *La Declaración Universal de Derechos Humanos.* Obtenido de Naciones Unidas: https://www.un.org/es/about-us/universal-declaration-of-human-rights

Pohle, J., & Van Audenhove, L. (2017). Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. *Media and Communication*, 1-6.

Range, L. (2021). *Case Study Methodologies.* Salem Press Encyclopedia of Health.

Rowan, D. (20 de Mar de 2014). *NSA at TED: 'arrogant' Snowden put lives at risk*. Obtenido de WIRED: https://www.wired.co.uk/article/nsa-ted

Sanger, D. (2017). A new age of ciberwarfare. En S. Khorana, J. Henrichsen, E. Bell, & T. Owen, *Journalism After Snowden: The Future of the Free Press in the Surveillance State* (págs. 186-196). New York: Columbia University Press.

Simmons, B. (2009). Women and international institutions: the effects of the Women's Convention on Female Education. En H. Milner, & A. Moravcsik, *Power, Interdependence, and Nonstate Actors in World Politics* (págs. 108-125). Princeton: Princeton University Press.

Solon, O. (31 de Jan de 2014). *David Cameron: 'I don't think Snowden's had an enormous public impact'*. Obtenido de WIRED: https://www.wired.co.uk/article/david-cameron-edward-snowden

Subramanian, R., & Katz, E. (2011). *The Global Flow of Information : Legal, Social, and Cultural Perspectives.* New York: New York University Press.

The Guardian. (14 de Jun de 2013). *Edward Snowden: Don't fly NSA whistleblower to UK, airlines told*. Obtenido de The Guardian: https://www.theguardian.com/world/2013/jun/14/dont-fly-edward-snowden-uk-airlines-told

The Guardian. (10 de Oct de 2013). *Patriot Act author prepares bill to put NSA bulk collection 'out of business'*. Obtenido de The Guardian: https://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill

The Guardian. (16 de Oct de 2013). *Snowden leaks: David Cameron urges committee to investigate Guardian*. Obtenido de The Guardian: https://www.theguardian.com/world/2013/oct/16/snowden-leaks-david-cameron-investigate-guardian

The New York Times. (7 de June de 2013). President Obama Defends N.S.A. Surveillance Programs. Estados Unidos. Obtenido de https://www.youtube.com/watch?v=m8F99BT8QAA

The New York Times. (13 de Jun de 2013). *U.S. preparing charges against leaker of data*. Obtenido de The New York Times: https://www.nytimes.com/2013/06/11/us/snowden-facing-charges-leaves-hong-kong-hotel.html

The New York Times. (2 de Jun de 2015). *U.S. Surveillance in place since 9/11 is sharply limited*. Obtenido de The New York Times:

https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html

The Transatlantic Digital Dialogue German Marshall Fund of the United States. (2015). *Transatlantic Digital Dialogue.* German Marshall Fund of the United States.

Timm, T. (10 de Aug de 2013). *Edward Snowden is a Patriot*. Obtenido de Politico: https://www.politico.com/story/2013/08/edward-snowden-is-a-patriot-095421

United States 114th Congress. (6 de June de 2015). H.R.2048 - USA FREEDOM Act of 2015. Washington DC. Obtenido de https://www.congress.gov/bill/114th-congress/house-bill/2048/text

Unver, A. (2018). *Politics of Digital Surveillance, National Security and Privacy.* Center for Economics and Foreign Policy Studies EDAM.

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022.* Cambridge: Harvard Kennedy School.

YouGov PLC. (16 de Jun de 2013). *Edward Snowden: Hero?* Obtenido de YouGov: https://yougov.co.uk/topics/politics/articles-reports/2013/06/16/edward-snowden-hero

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books.

Anexos

Anexo A: "Nuestro Compromiso De Proteger Su Información", De Marissa Mayer, Ceo De Yahoo![16]

Our Commitment to Protecting Your Information

by Marissa Mayer, Yahoo CEO

We've worked hard over the years to earn our users' trust and we fight hard to preserve it.

As you know, there have been a number of reports over the last six months about the U.S. government secretly accessing user data without the knowledge of tech companies, including Yahoo. I want to reiterate what we have said in the past: Yahoo has never given access to our data centers to the NSA or to any other government agency. Ever.

There is nothing more important to us than protecting our users' privacy. To that end, we recently announced that we will make Yahoo Mail even more secure by introducing https (SSL - Secure Sockets Layer) encryption with a 2048-bit key across our network by January 8, 2014.

Today we are announcing that we will extend that effort across ***all*** Yahoo products. More specifically this means we will:

- **Encrypt all information that moves between our data centers by the end of Q1 2014;**
- **Offer users an option to encrypt all data flow to/from Yahoo by the end of Q1 2014;**
- **Work closely with our international Mail partners to ensure that Yahoo co-branded Mail accounts are https-enabled**.

As we have said before, we will continue to evaluate how we can protect our users' privacy and their data. We appreciate, and certainly do not take for granted, the trust our users place in us.

[16] Se mantiene en idioma original para mantener fidelidad y evitar imprecisiones de traducción.

Anexo B: "Una Carta Abierta A Washington"[17]

An Open Letter to Washington

Dear Mr. President and Members of Congress,

We understand that governments have a duty to protect their citizens. But this summer's revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual – rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It's time for a change.

For our part, we are focused on keeping users' data secure – deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope.

We urge the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight.

To see the full set of principles we support, visit ReformGovernmentSurveillance.com

Sincerely,

AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo!

[17] Se mantiene en idioma original para mantener fidelidad y evitar imprecisiones de traducción.

Anexo C: Resumen de la ley 114-23 adoptada el 2 de junio de 2015 por el 114º congreso de los estados unidos, "Ley de libertad estadounidense"[18]

Public Law No: 114-23 (06/02/2015)

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015

TITLE I--FISA BUSINESS RECORDS REFORMS

(Sec. 101) Amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to establish a new process to be followed when the Federal Bureau of Investigation (FBI) submits an application to a FISA court for an order requiring the production of business records or other tangible things for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. (The FBI currently uses such authority to request FISA orders requiring telephone companies to produce telephone call records to the National Security Agency.)

Prohibits the FBI from applying for a tangible thing production order unless a specific selection term is used as the basis for the production. Maintains limitations under current law that prohibit the FBI from applying for tangible thing production orders for threat assessments.

Establishes two separate frameworks for the production of tangible things with different standards that apply based on whether the FBI's application seeks:

- production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation to protect against international terrorism, in which case the specific selection term must specifically identify an individual, account, or personal device; or
- production of call detail records or other tangible things in any other manner, in which case the selection term must specifically identify an individual, a federal officer or employee, a group, an entity, an association, a corporation, a foreign power, an account, a physical or an electronic address, a personal device, or any other specific identifier but is prohibited from including, when not used as part of a specific identifier, a broad geographic region (including the United States, a city, county, state, zip code, or area code) or an electronic communication or remote computing service provider, unless the provider is itself a subject of an authorized investigation.

Defines "call detail record" as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call. Excludes from such definition: (1) the contents

[18]Se mantiene en idioma original para mantener fidelidad y evitar imprecisiones de traducción.

of any communication; (2) the name, address, or financial information of a subscriber or customer; or (3) cell site location or global positioning system information.

Requires the FBI, in applications for ongoing production of call detail records for investigations to protect against international terrorism, to show: (1) reasonable grounds to believe that the call detail records are relevant to such investigation; and (2) a reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation for such terrorism.

Requires a judge approving such an ongoing release of call detail records for an investigation to protect against international terrorism to:

- limit such production to a period not to exceed 180 days but allow such orders to be extended upon application, with FISA court approval;
- permit the government to require the production of an initial set of call records using the reasonable, articulable suspicion standard that the term is associated with a foreign power or an agent of a foreign power and then a subsequent set of call records using session-identifying information or a telephone calling card number identified by the specific selection term that was used to produce the initial set of records (thus limiting the government to what is commonly referred to as two "hops" of call records); and
- direct the government to adopt minimization procedures requiring prompt destruction of produced call records that are not foreign intelligence information.

Allows a FISA court to approve other categories of FBI requests for the production of call detail records or tangible things (i.e., FBI call detail record and tangible thing applications that do not seek ongoing production of call detail records created before, on, or after the date of an application relating to an authorized investigation to protect against international terrorism) without subjecting the production to: (1) the reasonable, articulable suspicion standard for an association with a foreign power or an agent of a foreign power; (2) the 180-day or the two-hop limitation; or (3) the special minimization procedures that require prompt destruction of produced records only if the order approves an ongoing production of call detail records for investigations to protect against international terrorism.

(Sec. 102) Authorizes the Attorney General to require the emergency production of tangible things without first obtaining a court order if the Attorney General: (1) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing production can be obtained with due diligence, (2) reasonably determines that a factual basis exists for the issuance of such a production order, (3) informs a FISA judge of the decision to require such production at the time the emergency decision is made, and (4) makes an application to a FISA judge within seven days after the Attorney General requires such emergency production.

Terminates the authority for such emergency production of tangible things when the information sought is obtained, when the application for the order is denied, or after the

expiration of seven days from the time the Attorney General begins requiring such emergency production, whichever is earliest.

Prohibits information obtained or evidence derived from such an emergency production from being received in evidence or disclosed in any proceeding in or before any court, grand jury, agency, legislative committee, or other authority of the United States, any state, or any political subdivision if: (1) the subsequent application for court approval is denied, or (2) the production is terminated, and no order is issued approving the production. Bars information concerning any U.S. person acquired from such production from being used or disclosed in any other manner by federal officers or employees without the consent of such person, except with approval of the Attorney General if the information indicates a threat of death or serious bodily harm.

(Sec. 103) Requires FISA court orders approving the production of tangible things to include each specific selection term used as the basis for such production. Prohibits FISA courts from authorizing the collection of tangible things without the use of a specific selection term.

(Sec. 104) Requires a FISA court, as a condition to approving an application for a tangible thing production order, to find that the minimization procedures submitted with the application meet applicable FISA standards. Authorizes the court to impose additional minimization procedures.

Allows a nondisclosure order imposed in connection with a tangible thing production order to be challenged immediately by filing a petition for judicial review. (Currently, such a tangible thing nondisclosure order cannot be challenged until one year after the issuance of the production order.) Removes a requirement that a judge considering a petition to modify or set aside a nondisclosure order treat as conclusive a certification by the Attorney General, the Deputy Attorney General, an Assistant Attorney General, or the FBI Director that disclosure may endanger national security or interfere with diplomatic relations.

(Sec. 105) Extends liability protections to persons who provide information, facilities, or technical assistance for the production of tangible things. (Currently, liability protections are limited to persons who produce such tangible things.)

(Sec. 106) Requires the government to compensate a person for reasonable expenses incurred in producing tangible things or providing technical assistance to the government to implement production procedures.

(Sec. 108) Amends the USA PATRIOT Improvement and Reauthorization Act of 2005 to require the Inspector General of the Department of Justice to audit the effectiveness and use of FISA authority to obtain production of tangible things from 2012 to 2014, including an examination of whether minimization procedures adopted by the Attorney General adequately protect the constitutional rights of U.S. persons. Directs the Inspector General of the Intelligence Community, for the same 2012-2014 period, to assess: (1) the importance of such information to the intelligence community; (2) the manner in which such information was collected, retained, analyzed, and disseminated; and (3) the

adequacy of minimization procedures, including an assessment of any minimization procedures proposed by an element of the intelligence community that were modified or denied by the court.

Requires such Inspectors General to report to Congress regarding the results of such audit and assessment.

(Sec. 109) Requires amendments made by this Act to FISA's tangible thing requirements to take effect 180 days after enactment of this Act. Prohibits this Act from being construed to alter or eliminate the government's authority to obtain an order under the tangible things requirements of FISA as in effect prior to the effective date of such amendments during the period ending on such effective date.

(Sec. 110) Prohibits this Act from being construed to authorize the production of the contents of any electronic communication from an electronic communication service provider under such tangible thing requirements.

TITLE II--FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

(Sec. 201) Requires the government's FISA applications for orders approving pen registers or trap and trace devices to include a specific selection term as the basis for the use of the register or device. Prohibits broad geographic regions or an identification of an electronic communications service or a remote computing service from serving as such selection term.

(Sec. 202) Directs the Attorney General to ensure that appropriate privacy procedures are in place for the collection, retention, and use of nonpublicly available information concerning U.S. persons that is collected through a pen register or trap and trace device installed with FISA court approval.

TITLE III--FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

(Sec. 301) Limits the government's use of information obtained through an authorization by the Attorney General and the Director of National Intelligence (DNI) to target non-U.S. persons outside the United States if a FISA court later determines that certain targeting or minimization procedures certified to the court are unlawful.

Prohibits information obtained or evidence derived from an acquisition pursuant to a part of a targeting certification or a related minimization procedure that the court has identified as deficient concerning a U.S. person from being received in evidence or otherwise disclosed in any proceeding in or before any court, grand jury, agency, legislative committee, or other authority of the United States, any state, or any political subdivision.

Bars information concerning any U.S. person acquired pursuant to a deficient part of a certification from being used or disclosed subsequently in any other manner by federal officers or employees without the consent of the U.S. person, except with approval of the Attorney General if the information indicates a threat of death or serious bodily harm.

Allows a FISA court, if the government corrects the deficiency, to permit the use or disclosure of information obtained before the date of the correction.

TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

(Sec. 401) Directs the presiding judges of the FISA court and the FISA court of review to jointly designate at least five individuals to serve as amicus curiae to assist in the consideration of any application for an order or review that presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.

Permits FISA courts to appoint an individual or organization to serve as amicus curiae in other instances, including to provide technical expertise. Requires such amicus curiae to provide: (1) legal arguments that advance protection of individual privacy and civil liberties, or (2) other legal arguments or information related to intelligence collection or communications technology.

Allows the FISA court of review to certify a question of law to be reviewed by the Supreme Court. Permits the Supreme Court to appoint FISA amicus curiae or other persons to provide briefings or other assistance upon such a certification.

(Sec. 402) Requires the DNI to: (1) conduct a declassification review of each decision, order, or opinion issued by the FISA court or the FISA court of review that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of "specific selection term" as defined in this Act; and (2) make such decisions, orders, or opinions publicly available to the greatest extent practicable, subject to permissible redactions.

Authorizes the DNI to waive such review and public availability requirements if: (1) a waiver is necessary to protect the national security of the United States or properly classified intelligence sources or methods, and (2) an unclassified statement prepared by the Attorney General is made publicly available to summarize the significant construction or interpretation of law.

TITLE V--NATIONAL SECURITY LETTER REFORM

(Sec. 501) Amends the federal criminal code, the Right to Financial Privacy Act of 1978, and the Fair Credit Reporting Act to require the FBI and other government agencies to use a specific selection term as the basis for national security letters that request information from wire or electronic communication service providers, financial institutions, or consumer reporting agencies. Requires the government to identify: (1) a person, entity, telephone number, or account for requests for telephone toll and transactional records; (2) a customer, entity, or account when requesting financial records for certain intelligence or protective functions; or (3) a consumer or account when requesting consumer reports for counterintelligence or counterterrorism purposes.

Revises standards under which the government can prohibit recipients of national security letters from disclosing to anyone that the government has sought or obtained access to the requested information.

(Sec. 502) Directs the Attorney General to adopt procedures for imposed nondisclosure requirements, including requirements under the National Security Act of 1947, to be reviewed at appropriate intervals and terminated if facts no longer support nondisclosure.

Removes a requirement that the court treat as conclusive a certification by the Attorney General, the Deputy Attorney General, an Assistant Attorney General, or the FBI Director that disclosure may endanger U.S. national security or interfere with diplomatic relations.

(Sec. 503) Allows national security letter recipients to challenge national security letter requests or nondisclosure requirements under modified procedures for filing a petition for judicial review.

TITLE VI--FISA TRANSPARENCY AND REPORTING REQUIREMENTS

(Sec. 601) Requires the Attorney General to expand an annual report to Congress regarding tangible thing applications to include a summary of compliance reviews and the total number of: (1) applications made for the daily production of call detail records created before, on, or after the date of an application relating to an authorized investigation to protect against international terrorism; and (2) orders approving such requests.

Directs the Attorney General to report to Congress annually regarding tangible things applications and orders in which the specific selection term does not specifically identify an individual, account, or personal device. Requires the report to indicate whether the court approving such orders has directed additional, particularized minimization procedures beyond those adopted by the Attorney General.

(Sec. 602) Directs the Administrative Office of the U.S. Courts to submit annually to Congress the number of: (1) FISA applications submitted, and orders granted, modified, or denied under specified FISA authorities; and (2) appointments of an individual to serve as amicus curiae for FISA courts, including the name of each appointed individual, as well as any findings that such an appointment is not appropriate. Makes the report subject to a declassification review by the Attorney General and the DNI.

Directs the DNI to make available publicly a report that identifies, for the preceding 12-month period, the total number of: (1) FISA court orders issued for electronic surveillance, physical searches, the targeting of persons outside the United States, pen registers and trap and trace devices, call detail records, and other tangible things; and (2) national security letters issued.

Requires the DNI's reports to include the estimated number of: (1) targets of certain FISA orders, (2) search terms and queries concerning U.S. persons when the government retrieves information from electronic or wire communications obtained by targeting non-U.S. persons outside the United States, (3) unique identifiers used to communicate certain collected information, and (4) search terms concerning U.S. persons used to query a database of call detail records. Exempts certain queries by the FBI from such estimates.

(Sec. 603) Permits a person who is subject to a nondisclosure requirement accompanying a FISA order, directive, or national security letter to choose one of four methods to report publicly, on a semiannual or annual basis, the aggregate number of orders, directives, or letters with which the person was required to comply. Specifies the categories of orders, directives, and letters to be itemized or combined, the details authorized to be included with respect to contents or noncontents orders and the number of customer selectors targeted, and the ranges within which the number of orders, directives, or letters received may be reported aggregately in bands under each permitted method (i.e., reported in bands of 1000, 500, 250, or 100 depending on the chosen method).

Requires the information that may be included in certain aggregates to be delayed by 180 days, one year, or 540 days depending on the chosen reporting method and whether the nondisclosure requirements are contained in a new order or directive concerning a platform, product, or service for which the person did not previously receive an order or directive.

(Sec. 604) Expands the categories of FISA court decisions, orders, or opinions that the Attorney General is required to submit to Congress within 45 days after issuance of the decision to include: (1) a denial or modification of an application under FISA; and (2) a change of the application, or a novel application, of any FISA provision. (Currently, the Attorney General is only required to submit only decisions regarding a significant construction or interpretation of any FISA provision.)

(Sec. 605) Revises reporting requirements regarding electronic surveillance, physical searches, and tangible things to include the House Judiciary Committee as a recipient of such reports.

Requires the Attorney General to identify in an existing semiannual report each agency on behalf of which the government has applied for orders authorizing or approving the installation and use of pen registers or trap and trace devices under FISA.

TITLE VII--ENHANCED NATIONAL SECURITY PROVISIONS

(Sec. 701) Establishes procedures for a lawfully authorized targeting of a non-U.S. person previously believed to be located outside the United States to continue for a period not to exceed 72 hours from the time that the non-U.S. person is reasonably believed to be located inside the United States. Requires an element of the intelligence community, as a condition to exercising such authority, to: (1) determine that a lapse in the targeting poses a threat of death or serious bodily harm; (2) notify the Attorney General; and (3) request, as soon as practicable, the employment of emergency electronic surveillance or emergency physical search under appropriate FISA standards.

(Sec. 702) Expands the definition of "agent of a foreign power" to include a non-U.S. person who: (1) acts in the United States for or on behalf of a foreign power engaged in clandestine intelligence activities in the United States contrary to U.S. interests or as an officer, employee, or member of a foreign power, irrespective of whether the person is inside the United States; or (2) knowingly aids, abets, or conspires with any person

engaging in an international proliferation of weapons of mass destruction on behalf of a foreign power or conducting activities in preparation for such proliferation.

(Sec. 704) Increases from 15 to 20 years the maximum penalty of imprisonment for providing material support or resources to a foreign terrorist organization in cases where the support does not result in the death of any person.

(Sec. 705) Amends the USA PATRIOT Improvement and Reauthorization Act of 2005 and the Intelligence Reform and Terrorism Prevention Act of 2004 to extend until December 15, 2019, FISA authorities concerning: (1) the production of business records, including call detail records and other tangible things; (2) roving electronic surveillance orders; and (3) a revised definition of "agent of a foreign power" that includes any non-U.S. persons who engage in international terrorism or preparatory activities (commonly referred to as the "lone wolf" provision). (Currently, such provisions are scheduled to expire on June 1, 2015.)

TITLE VIII--SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A--Safety of Maritime Navigation

(Sec. 801) Amends the federal criminal code to provide that existing prohibitions against conduct that endangers the safe navigation of a ship: (1) shall apply to conduct that is committed against or on board a U.S. vessel or a vessel subject to U.S. jurisdiction, in U.S. territorial seas, or by a U.S. corporation or legal entity; and (2) shall not apply to activities of armed forces during an armed conflict or in the exercise of official duties.

Sets forth procedures regarding the delivery of a person who is suspected of committing a maritime navigation or fixed platform offense to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.

Subjects property used or intended to be used to commit or to facilitate the commission of a maritime navigation offense to civil forfeiture.

(Sec. 802) Prohibits: (1) using in or on a ship or a maritime fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon, or other nuclear explosive device in a manner likely to cause death or serious injury or damage when the purpose is to intimidate a population or to compel a government or international organization to act or abstain from acting; (2) transporting on board a ship such material or device (or certain related material or technology) that is intended for such use, with specified exceptions; (3) transporting on board a ship a person known to have committed a maritime navigation offense intending to assist such person to evade prosecution; (4) injuring or killing any person in connection with such an offense; or (5) conspiring, attempting, or threatening to commit such an offense. Sets forth: (1) the circumstances in which the United States can exercise jurisdiction over such offenses, and (2) exceptions applicable to activities of the armed forces. Provides for civil forfeiture of property used to commit or to facilitate a violation.

(Sec. 805) Includes offenses involving violence against maritime navigation and maritime transport involving weapons of mass destruction within the definition of "federal crime of terrorism."

Subtitle B--Prevention of Nuclear Terrorism

(Sec. 811) Prohibits anyone, knowingly, unlawfully, and with intent to cause death, serious bodily injury, or substantial damage to property or the environment, from: (1) possessing radioactive material or making or possessing a nuclear explosive device or a radioactive material dispersal or radiation-emitting device; (2) using radioactive material or a device, using, damaging, or interfering with the operation of a nuclear facility in a manner that causes or increases the risk of the release of radioactive material, or causing radioactive contamination or exposure to radiation; or (3) threatening, attempting, or conspiring to commit such an offense. Sets forth: (1) the circumstances in which the United States can exercise jurisdiction over such offenses, and (2) exceptions applicable to activities of the armed forces.

Includes such offenses within the definition of "federal crime of terrorism."

(Sec. 812) Amends provisions prohibiting transactions involving nuclear materials to: (1) prohibit, intentionally and without lawful authority, carrying, sending, or moving nuclear material into or out of a country; and (2) establish an exception for activities of the armed forces.