CUADERNOS DE INVESTIGACIÓN

# Funciones e instrumentos de inteligencia al servicio de los intereses de seguridad de Estados Unidos

## Programas de vigilancia masiva de la National Security Agency,

## ¿Razón de Estado?

Enrique Utrilla Quintanar
Director: Soledad Segoviano Monterrubio

CI 23/2016
ISSN: 2530-3570

Universidad Complutense de Madrid
Facultad de Ciencias Políticas y Sociología

# Índice


**1. Introducción. ..... 6**
1.1. Delimitación del tema y objetivos. ..... 6
1.2. Metodología y fuentes. ..... 8
1.3. Hipótesis. ..... 10
1.4. Marco teórico y aproximación conceptual. ..... 11

**2. La construcción de la maquinaria de inteligencia norteamericana. ..... 18**
2.1. La National Security Act. Erigiendo la estructura de inteligencia. [1947] ..... 18
2.2. De la Armed Forces Security Agency a la National Security Agency. [1949-1952] ..... 20

**3. La National Security Agency: Etapas en la configuración del centinela global. ..... 21**
3.1. La NSA en la Guerra Fría. [1952-1991] ..... 21
3.1.1. El antecedente de la vigilancia: El Counter Intelligence Program. [1956-1971] ..... 21
3.1.2. La National Reconnaissance Office (NRO). Comienzo de las rivalidades entre Agencias Ejecutivas de vigilancia. [1961] ..... 23
3.1.3. Creación del Central Security Service. El complemento funcional de la NSA. ..... 24
3.1.4. El Church Committee: Las revelaciones de los programas MINARET y ..... 24
3.1.5. La Foreign Intelligence Surveillance Act (FISA). El mecanismo supervisor de inteligencia. [1978] ..... 26
3.1.6. La era del criptosecretismo: La NSA e IBM. El algoritmo Data Encryption Standard. [1970-1979] ..... 27
3.1.7. La Orden Ejecutiva 12333. Las 16 Agencias Ejecutivas de inteligencia. [1981] ..... 29
3.1.8. La Goldwater-Nichols Act. La reorganización del Department of Defense. [1986] ..... 30
3.2. La NSA en la post-Guerra Fría. [1991-2001] ..... 32
3.2.1. El dividendo de la paz en la etapa Clinton y la puesta en marcha de la Revolution in Military Affairs. El impacto en la vigilancia del siglo XXI. [1993-2001] ..... 32
3.3. La NSA en el siglo XXI. Del 11-S a las revelaciones de Edward Snowden. [2001- 2013] ..... 34
3.3.1. Administración George W. Bush. [2001-2009] ..... 34
3.3.2. Administración Barack Obama. [2009-Actualidad] ..... 44

**4. El desafío de las filtraciones en la comunidad de inteligencia norteamericana ..... 50**
4.1. Filtradores y filtraciones anteriores a WikiLeaks. ..... 50
4.2. WikiLeaks. La ventana a las revelaciones masivas. ..... 56
4.3. Filtraciones más relevantes de WikiLeaks. ..... 57
4.4. Edward Snowden. ¿Héroe o traidor? ..... 59

**5. Programas de espionaje masivo de la NSA revelados por Edward Snowden. ..... 61**
5.1. Tratado UKUSA. Construyendo la estructura de espionaje. El club de "Los Cinco Ojos". ..... 61
5.2. Clasificación de los objetivos de espionaje. El impulso de la cooperación y la ausencia de amistades en el entorno global. ..... 63
5.3. Programa PRISM. ..... 64
5.4. Programa BOUNDLESS INFORMANT. ..... 66
5.5. Programa SHELLTRUMPET. ..... 68
5.6. Programa X-KEYSCORE. ..... 68

5.7. Programa PROJECT BULLRUN. ..... 70
5.8. Programas Upstream Collection. ..... 71
5.8.1. Programa STORMBREW. ..... 71
5.8.2. Programa OAKSTAR. ..... 72
5.8.3. Programa BLARNEY. ..... 74
5.8.4. Programa FAIRVIEW. ..... 75
5.9. La Estrecha colaboración con el Government Communications Headquarters (GCHQ) británico. ..... 77
5.9.1. Programa OPTIC NERVE. ..... 77
5.9.2. Programa THIEVING MAGPIE. ..... 78
5.9.3. Programa TEMPORA. ..... 79

**6. Análisis de impacto de las revelaciones de Edward Snowden. ..... 81**
6.1. Ámbito interno de Estados Unidos. ..... 81
6.2. Panorama internacional. ..... 82
6.2.1. Naciones Unidas frente a los programas de la NSA. La acción diplomática de Brasil y Alemania. ..... 82
6.2.2. El Parlamento Europeo: Comisión de Libertades Civiles, Justicia y Asuntos de Interior. [21/02/14] ..... 84
6.2.3. Reacciones por países: ..... 84
6.3. Reacciones de otros observadores: Human Rights Watch y American Civil Liberties Union. . 89

**7. Conclusiones. ..... 92**

**8. BIBLIOGRAFÍA ..... 95**

**9. ANEXO APÉNDICES ..... 104**
9.1. APÉNDICE A: ..... 105
9.2. APÉNDICE B: ..... 111
9.3. APÉNDICE C: ..... 115
9.4. APÉNDICE D: ..... 124
9.5. APÉNDICE E: ..... 129
9.6. APÉNDICE F: ..... 134
9.7. APÉNDICE G: ..... 139
9.8. CRONOLOGÍA DE ACONTECIMIENTOS ..... 143

**RESUMEN**

La comunidad de inteligencia norteamericana ha experimentado profundas mutaciones con objeto de adaptarse a las diferentes dinámicas y desafíos internacionales. No obstante, han sido dos los acontecimientos que han supuesto un punto de inflexión en su adaptación a la coyuntura global. Por un lado, la confrontación bipolar y el cuestionamiento de liderazgo estadounidense por parte de la URSS durante la Guerra Fría. Por el otro, los ataques terroristas del 11 de septiembre de 2001. Frente al primer escenario, la Administración Truman respondió con la aprobación de la *National Security Act* de 1947, sobre la que se fue conformando la comunidad de inteligencia norteamericana, readaptada otras tantas veces con motivo de las diferentes crisis internacionales y con el objetivo prioritario de garantizar la seguridad nacional en un entorno internacional adverso. En cuanto al segundo escenario, ya en el siglo XXI, la Administración George W. Bush reaccionó a través de una Ley que ayudara al Gobierno a tener controlada cualquier posible amenaza: la *USA PATRIOT ACT*. Un contexto de *Global War on Terror* donde la seguridad dependiente de las actividades de inteligencia quedaba subordinada a la razón de Estado, mediante un criterio de finalidad antiterrorista para justificar cualquier medio utilizado. Una etapa marcada por la cuestionable eficacia del *United States Foreign Intelligence Surveillance Court,* el camino hacia la *FISA Amendments Act* de 2008 mediante las reformas de 2006 y 2007 o el continuismo de la Administración Obama con la actual *USA FREEDOM ACT*.

En la historia de la comunidad de inteligencia norteamericana, sus recurrentes casos de filtración interna han demostrado la supeditación de las exigencias democráticas frente al interés prioritario derivado de la seguridad nacional. Los programas de vigilancia masiva de la *National Security Agency* revelados al diario *The Guardian* por el ex analista Edward Snowden son la demostración de cómo la vigilancia global al servicio de los intereses globales de Estados Unidos abarca ámbitos comerciales y políticos más allá de los planes antiterroristas a la vez que involucra a corporaciones empresariales y vulnera libertades y derechos democráticos, sin importar la respuesta ambigua de un panorama internacional que a la vez que condena la vigilancia de la *NSA* coopera con esta Agencia.

**Palabras clave**: *Comunidad de inteligencia, Democracia, Edward Snowden, Espionaje, Inteligencia, NSA, Programas de inteligencia, Seguridad, Terrorismo, Vigilancia global, 11-S.*

# 1. Introducción.

## 1.1. Delimitación del tema y objetivos.

El tema del presente Trabajo de Fin de Máster es la alarmante situación de vigilancia global impulsada por la *National Security Agency* (*NSA*) a raíz de los ataques terroristas del 11 de septiembre de 2001. La investigación persigue conocer de cerca la progresiva conformación de la comunidad de inteligencia norteamericana a partir de su nacimiento con la *National Security Act* de 1947, para comprender en qué momentos y a través de qué herramientas se ha producido el salto definitivo hacia el Estado de vigilancia masiva. El objetivo del trabajo es también dar cabida al conjunto de revelaciones del ex analista de la *NSA*, Edward Snowden, en junio de 2013, y que han hecho tambalear los cimientos de la propia comunidad de inteligencia norteamericana, tratando de medir el impacto de estas revelaciones tanto en el ámbito interno de Estados Unidos como en el contexto internacional.

El trabajo constará de seis partes o capítulos. En el primero, abordaremos la construcción de la maquinaria de inteligencia norteamericana y, para ello, tomaremos como punto de partida la aprobación, en julio de 1947, de la *National Security Act*. Por medio de este texto, la Administración del Presidente Harry S. Truman no solo proveerá al Gobierno norteamericano de un organismo clave en el asesoramiento presidencial en materia de seguridad nacional, como lo es el *National Security Council* (*NSC*), o de la *Central Intelligence Agency* (*CIA*) en sustitución de la *Office of Strategic Services* (*OSS*) anterior, sino que proporcionará un primer paso integral para garantizar la seguridad futura de los Estados Unidos. No hay que olvidar que la garantía de seguridad resultaba apremiante debido a la configuración de un nuevo orden internacional en el que la Unión Soviética ponía en duda el liderazgo global norteamericano. De la misma manera, como nuestro objeto de investigación se orienta a los programas de vigilancia de la *NSA*, daremos cabida en este primer apartado a la creación de esta Agencia. En este sentido, expondremos el contexto y las causas fundamentales que justifican la desaparición de la *Armed Forces Security Agency* (*AFSA*) en 1951 y el establecimiento de la *NSA* en su lugar a partir de 1952.

En el segundo capítulo, trataremos de abordar el proceso de conformación de la *NSA* en tres etapas a la vez que se desarrolla y fundamenta la comunidad de inteligencia norteamericana. En la primera etapa, explicaremos el período de la Guerra Fría comprendido entre 1952 y 1991. En este epígrafe daremos cabida como punto de arranque al programa *COINTELPRO*, antecedente en la vigilancia masiva impulsado por el *Federal Bureau of Investigation* (*FBI*), pero también se mostrará la creación de Agencias como la *National Reconnaissance Office* (*NRO*), cuyo papel es esencial en el avance de la vigilancia electrónica posterior, dadas sus capacidades tecnológicas; y el *Central Security Service (CSS*), como complemento criptográfico de la *NSA* desde 1972. De la misma manera, en este período incluiremos las investigaciones del *Church Committee,*

desarrolladas entre 1974 y 1976, y que implicaron la revelación de programas como *MINARET*, activo desde 1969 o *SHAMROCK*, desde 1945, vinculados a la *NSA*. Finalmente, aludiremos a la relevancia de la *Foreign Intelligence Surveillance Act* de 1978 como medida de control de las actividades de inteligencia a raíz de las investigaciones del *Church Committee* y a la articulación de la comunidad de inteligencia que llega hasta nuestros días, de la mano de la Orden Ejecutiva 12333, firmada por la Administración Reagan, en 1981, y que reconoce en el espionaje, el terrorismo y las armas de destrucción masiva, los núcleos de acción fundamentales. Como punto de enlace con el período de la post-Guerra Fría dedicaremos un apartado a la *Goldwater-Nichols Act* de 1986, que supuso la reorganización más importante del *Department of Defense* (*DoD*) desde su creación, con el convencimiento de muchos de los legisladores más influyentes acerca de la inoperancia y la ineficacia del *DoD* viendo el desarrollo traumático de la guerra de Vietnam.

En la segunda etapa, de la post-Guerra Fría, (1991-2001) abarcaremos dos aspectos fundamentales que tuvieron lugar durante la Administración Clinton: el dividendo de la paz y la *Revolution in Military Affairs* (*RMA*). En el caso del primero, nos ocuparemos de la etapa de crecimiento económico de los Estados Unidos debido al proceso de desmilitarización tras la caída del bloque comunista. En el caso de la *RMA*, la victoria norteamericana en la guerra del golfo pérsico, iniciada en agosto de 1991 y finalizada en febrero de 1992, supuso un punto de inflexión a la hora de participar en conflictos internacionales y en una clara apuesta por invertir el crecimiento económico en el aumento de las tecnologías disponibles en manos de los diferentes servicios militares.

Por último, en la última etapa abordaremos la perspectiva desde las dos últimas Administraciones norteamericanas: La Administración George W. Bush y la Administración Barack Obama. En la presidencia Bush (2001-2009) detallaremos los cambios funcionales en la seguridad e inteligencia norteamericana a raíz del 11-S, como han sido: La *USA PATRIOT ACT* de 2001, los fallos reconocidos en el *9/11 Commission Report* de 2004, el impacto de la *Intelligence Reform and Terrorism Prevention Act* de ese mismo año, el intento de revisión de la *USA PATRIOT ACT* de julio de 2005, el camino hacia la *FISA Amendments Act* de 2008 mediante las reformas de 2006 y 2007 (*Terrorist Surveillance Act*, *Electronic Surveillance Modernization Act y Protect America Act*) y finalmente la *Comprehensive National Cybersecurity Initiative*, que pone el acento en la ciberseguridad nacional. También mencionaremos el escándalo destapado por *USA Today* y que involucraba a las compañías de telecomunicaciones *AT&T*, *Verizon* y *BellSouth* con la *NSA* y que marcó un antes y un después en la revelación periodística de las prácticas de la Agencia.

Por su parte, en la Administración Obama (2009-Actualidad) destacaremos la ambivalencia en el discurso del Presidente comparando su discurso crítico como candidato, frente a la política de justificación de la vigilancia del Gobierno una vez asumido el cargo, en su comparecencia

pública ante los medios del 17 de enero de 2014 en respuesta a las revelaciones de Edward Snowden.

Nos detendremos en el verdadero papel que juega el *United States Foreign Intelligence Surveillance Court*, más plegado al servilismo que a la centinela sobre las Agencias de inteligencia, en especial de la *NSA*. Por último, trataremos de contestar a una sencilla pregunta, la *USA FREEDOM ACT* que releva a la *USA PATRIOT ACT* desde el 1 de junio de 2015, ¿se trata de un triunfo de Snowden o de una argucia política que aboga por el continuismo de la vigilancia?

En el tercer capítulo del trabajo, una vez precisada la comunidad de inteligencia norteamericana en sus diferentes etapas y dentro de ella, la *NSA*, cambiaremos el foco de atención hacia la filtración como fenómeno de oposición a las actividades de inteligencia del Gobierno norteamericano, lo que nos será útil para construir el camino hacia la figura de Edward Snowden. En la historia de la comunidad de inteligencia norteamericana son recurrentes, casi desde sus orígenes, los casos de filtración de información secreta o el surgimiento, como fuentes de oposición, de antiguos analistas o colaboradores de las Agencias de inteligencia estadounidense. Así, aludiremos a filtraciones de figuras como: Daniel Ellsberg, Ray McGovern, Coleen Rowley, Ronald William Pelton, Russ Tice, Thomas Tamm o Bradley Manning, entre otros.

Tras ellos, elaboraremos un breve perfil de *WikiLeaks*, que también se ha erigido en una fuente de filtración de actividades del Gobierno norteamericano desde que comenzara su actividad en 2001. En este sentido, aludiremos a sus filtraciones más importantes, como son: el *Baghdad airstrike*, la Guerra de Afganistán, la Guerra de Irak, el *Cablegate* y el *Global Intelligence Files leak*. Finalmente hablaremos sobre Edward Snowden: Quién es y cuáles son las verdaderas motivaciones que le guían para llevar

a cabo las revelaciones, pero sobre todo trataremos de responder a la pregunta ¿Héroe o traidor?

En el cuarto capítulo trataremos de abordar el aspecto más técnico de la investigación: los programas de inteligencia de la *NSA* revelados por Snowden. Por razones lógicas, en esta investigación no se incluyen todos los programas revelados debido a las limitaciones que deben respetarse en materia de presentación, sin embargo, los programas de inteligencia que aquí aparecen recogidos son los que más visibilidad y eco han tenido entre la opinión pública, medios de comunicación y Gobiernos, así como observadores y organismos civiles internacionales. Estos son: *PRISM*, *BOUNDLESS INFORMANT, SHELLTRUMPET, X-KEYSCORE, PROJECTBULLRUN, STORMBREW, OAKSTAR, BLARNEY* y *FAIRVIEW*. Es importante

también mencionar programas como *OPTIC NERVE, THIEVING MAGPIE* y *TEMPORA*, estos últimos demostrarán la estrecha cooperación entre la *NSA* y el *Government Communications Headquarters* (*GCHQ*) británico.

Finalmente, en el quinto capítulo abarcaremos el impacto que las revelaciones sobre la vigilancia global de la *NSA* han tenido a nivel nacional, en Estados Unidos, desde las perspectivas social, legislativa y ejecutiva, y en el contexto internacional, donde aludiremos a iniciativas relevantes como la Resolución contra el espionaje de la *NSA* en la Asamblea General de la *ONU* y a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo. No obstante, en un intento de profundizar en el impacto de tales revelaciones, abordaremos las reacciones internacionales por países (los que se han visto más afectados) y estos serán: Alemania, Australia, Brasil, Canadá, España, Francia, México, Reino Unido, y Rusia.

Desde esta perspectiva por ejemplo comentaremos como breves píldoras informativas, la participación activa en el espionaje del servicio de inteligencia exterior alemán así como de la Agencia especializada en inteligencia electrónica de Australia. El impulso en Brasil de la Comisión de Investigación Parlamentaria "*CPI da Espionagem*". La postura de la *Canadian Civil Liberties Association* en respuesta a la cooperación de su Gobierno con la *NSA*. La suministración del Centro Nacional de Inteligencia de España a la *NSA* de hasta 60 millones de registros de llamadas de españoles entre diciembre de 2012 a enero de 2013. Las medidas introducidas en el sistema legal francés orientadas al "*geo-tracking*", es decir, a limitar la capacidad de las Agencias de vulnerar la privacidad debido a la localización de civiles por medio de sus teléfonos móviles. El activismo opositor en México de las ONG *ContingenteMX* y *SonTusDatos*. La excesiva falta de control del Gobierno británico sobre sus servicios de inteligencia y el deterioro de las relaciones entre Estados Unidos y Rusia después de que Moscú amparase y reconociese a Edward Snowden el derecho de asilo en su país.

Para terminar, recogeremos la postura de dos observadores globales. Por un lado *Human Rights Watch,* que constituye una fuente relevante de investigación debido a sus disertaciones sobre el Estado de vigilancia norteamericano y su impacto internacional, tanto en los Informes de 2014 como de 2015 así como en el recién publicado Informe de 2016. Por otro lado, aludiremos también a la *American Civil Liberties Union* (*ACLU*), porque servirá para tener un punto de vista autóctono de lo que han significado las revelaciones de Snowden.

En el sexto y último capítulo crearemos un espacio de reflexión que servirá de modo conclusivo para refutar, o no, las hipótesis de la presente investigación.

## 1.2. Metodología y fuentes.

Resulta necesario partir de una premisa en la realización de este Trabajo: La función de inteligencia siempre se ha visto justificada desde el nacimiento de Estados Unidos como nación ante la necesidad de garantizar las más necesarias y fundamentales condiciones de seguridad frente a peligros proce-

dentes del ámbito internacional. No obstante, después de la II Guerra

Mundial, coincidiendo con la supremacía de la corriente doctrinal del Realismo político,[1] la inteligencia tornó a convertirse en instrumento esencial de la política exterior y de seguridad nacional de Estados Unidos.

Para la realización de este Trabajo se ha empleado ante todo un método de investigación: el deductivo. Tal como señala Rafael Calduch, para emplear este método se hace necesario el empleo de otros métodos como el *"descriptivo, analítico y comparativo, porque sólo gracias a ellos podemos establecer la analogía o correspondencia lógica y fenomenológica entre ley general y suceso particular"*.[2] De esta manera, se ha decidido que en la investigación estarán presentes, del mismo modo, los métodos: analítico, descriptivo e histórico-comparativo.

El método analítico nos ayudará a conocer mejor la realidad que conforma en la actualidad la comunidad de inteligencia partiendo desde la perspectiva de las diferentes etapas a las que se alude en el Trabajo, tanto en la Guerra Fría, como en la post-Guerra Fría así como en el escenario que presenta la *NSA* en el siglo XXI. En especial, el análisis es una faceta de estudio muy importante de cara a la extracción de los aspectos más relevantes de los diferentes documentos jurídicos que aparecerán en el Trabajo, por ejemplo de la Sección 215 de la *USA PATRIOT ACT* de 2001 o la Sección 702 de la *FISA Amendments Act* de 2008.

El método descriptivo facilitará una mejor comprensión de un escenario nada fácil de comprender, como es el de la comunidad de inteligencia norteamericana, pero en especial, cuando abordemos las características técnicas de los programas de vigilancia masiva de la *NSA* a los que nos referimos en este Trabajo. De la misma manera, tomar el pulso a las diferentes reacciones internacionales tras las revelaciones del espionaje norteamericano, requerirán de esfuerzos descriptivos debido a las diferentes repuestas de cada Gobierno, sociedad civil, observador global o movimiento ciudadano involucrado.

La aplicación del método histórico-comparativo nos proporcionará el hilo conductor de la sucesión cronológica que nos ayudará a adentrarnos en el análisis de la evolución de la política de inteligencia de Estados Unidos, especialmente desde la *National Security Act* y de los progresivos pasos que se dan hacia adelante en la conformación de una comunidad de inteligencia, y más concretamente de una Agencia (*NSA*), orientadas a la sospecha global. Es este eje cronológico el que nos permitirá establecer el marco deductivo generalizado en todo el Trabajo, pues partiremos de la comunidad de inteligencia para estudiar la *NSA* así como ofreceremos un contexto histórico sobre las filtraciones más conocidas que afectan al Gobierno norteamericano para acabar con la figura de Edward Snowden.

De la misma forma, en el Trabajo también tendrá cabida el método dialéctico en la medida en que se planteará el debate que enfrenta a las exigencias propias de regímenes democráticos frente las aspiraciones de seguridad de un Estado, toda vez que la consecución de la seguridad estatal absoluta constituye más una utopía que una realidad.

Por último, en relación al trabajo realizado con las fuentes, se buscará atender tanto a documentos oficiales de Estados Unidos, ya sea por medio de memorándums presidenciales a las conclusiones del *Church Committee* u Órdenes Ejecutivas, Leyes, la propia Constitución de los Estados Unidos o el Informe de la Comisión sobre el 11-S, entre otros. También utilizaremos obras de autores relevantes en el escenario de la inteligencia norteamericana como es el caso de Sherman Kent o James Bamford. No obstante, resulta relevante reflejar que habrá una

1 Escuela de pensamiento que contemplaba la realidad internacional como un entorno conflictivo, en el que prevalecían las relaciones de poder.
2 CALDUCH CERVERA, Rafael: *Métodos y técnicas de investigación en Relaciones Internacionales*, Ed: Universidad Complutense de Madrid, 2003, p. 34.

obra que tendrá mayor presencia que otras en el Trabajo, esta es: "*Snowden: Sin un lugar donde esconderse*", escrita por Glenn Greenwald, periodista de *The Guardian* al que Snowden reveló las actividades de la *NSA* en junio de 2013, y que constituye por ello, una prueba documental importante para la realización de la investigación. También constituyen valor de fuente, los recursos en vídeo o documental, como el discurso de Obama de enero de 2014 o el documental "*Citizenfour*" y la posición con relación al tema de investigación de observadores globales o *Think Tanks* como: *Canadian Journalists for Free Expression*, *Congressional Research Service* o *Center for Security Policy*, entre otros. En este sentido, también se consultarán fuentes especializadas en el tratamiento de actividades de inteligencia norteamericana, como pueden ser *The Wire* o *The Intercept*.

Del mismo modo también serán de obligada consulta fuentes relacionadas con Organizaciones Internacionales Gubernamentales y Organizaciones No Gubernamentales. En el caso del primero, Naciones Unidas o el Parlamento Europeo serán fundamentales, mientras que en el caso del segundo, *Human Rights Watch*, *American Civil Liberties Union* o la *British Columbia Civil Liberties Association*.

Por último, en tanto que las revelaciones de Snowden se han llevado a cabo en el diario británico *The Guardian* y han abierto una hemorragia periodística a la hora de revelar secretos gubernamentales, los propios medios de comunicación constituirán también un valor de fuente esencial en la realización de este trabajo. No cabe duda de que la perspectiva periodística habrá de estar presente más si cabe cuando una de las líneas de investigación del Trabajo supone evaluar la calidad de la democracia en la que vivimos.

### 1.3. Hipótesis.

Las principales hipótesis que se intentan verificar con esta investigación son las siguientes:

1). Las actividades de inteligencia norteamericanas ya no son un mero recurso con objeto de anticipar amenazas que puedan poner en peligro la seguridad de la nación, sino que en ellas subyace siempre una **razón de Estado**, es decir, la participación activa del Gobierno en la toma de decisiones ayudando a legitimar posibles vulneraciones de Leyes o derechos humanos. Esto es así gracias a la política de la negación plausible (*plausible denial*). Mediante esta política, tanto el Presidente como funcionarios de alto rango del Gobierno norteamericano, quedan protegidos frente a posibles escándalos en caso de que operaciones o programas de vigilancia lleguen a conocerse. Les permite negar toda responsabilidad sin ser acusados de perjurio, evadiendo así cualquier situación política verdaderamente comprometida.

El reordenamiento de las relaciones internacionales a raíz de la caída del bloque soviético ha obligado al Gobierno de los Estados Unidos a reconfigurar sus actividades de inteligencia de tal modo que la vigilancia heredada de la Guerra Fría se ha reorientado al ámbito civil para obtener los máximos datos posibles de cara a la detección y reacción temprana frente a hostilidades. Aunque con ello se ejecuten labores de vigilancia sobre civiles que para nada constituyen núcleo de sospecha.

2). Los diferentes mecanismos y herramientas tales como la *Foreign Intelligence Surveillance Act* de 1978 así como el *Foreign Intelligence Surveillance Court*, nacidos a raíz de las investigaciones del *Church Committee* con objeto de vigilar las actividades de inteligencia y ubicar límites en los abusos de poder y extralimitación de funciones de las Agencias, no han servido con el tiempo sino para facilitar un clima de **servilismo y concesión** plegado una vez más a las razones de Estado que se esgrimen por parte del Ejecutivo y en ocasiones, con la connivencia del Congreso, para legitimar las prácticas de vigilancia.

3). Durante la Administración Obama la justificación de la existencia de los programas de vigilancia masiva desarrollados por la *NSA* ha sido la lucha frente a la amenaza terrorista global. No obstante, el progreso tecnológico y la mejora de las capacidades de recogida y almacenamiento al alcance de la Agencia han posibilitado que **sus programas se hayan utilizado también para adquirir ventajas comerciales así como ventajas políticas o de negociación**. Desde esta perspectiva, parece que la vigilancia masiva del Gobierno norteamericano utilice el **planteamiento del terrorismo para abarcar ámbitos de influencia económica y política** al margen de la lucha contra los terroristas.

4). Las revelaciones del ex analista de la *NSA* Edward Snowden han contribuido a avivar el debate sobre los límites de un Estado para garantizar su seguridad nacional pero también la proyección global e internacional de su seguridad. El Gobierno norteamericano al referirse a la figura de Snowden, lo presenta como un traidor que ha contribuido con sus revelaciones a debilitar el sistema de seguridad de Estados Unidos, poniendo en peligro tanto métodos como personal y fuentes de la comunidad de inteligencia y facilitando de esta manera la anticipación de los servicios de inteligencia rivales así como el trabajo de células terroristas preparadas para atacar. No obstante, resulta **legítima la denuncia de Snowden** si en el ejercicio de la protección nacional se vulneran principios democráticos tales como el derecho a la intimidad, la privacidad o las libertades de reunión o asociación.

5). Tras las revelaciones de Edward Snowden acerca de los programas de vigilancia de la *NSA*, diferentes organizaciones internacionales como Naciones Unidas o el Parlamento Europeo han pedido respuestas a Estados Unidos sin que ello se haya visto traducido, por el momento, en una política activa de suspensión de tales actividades. En el contexto internacional, se han observado reacciones de rechazo a la vigilancia de la *NSA*; sin embargo, esos mismos países, como Alemania, España, Brasil, etcétera, son los que han negado el asilo a Snowden cuando lo ha solicitado o incluso no se atreven a condenar activamente la vigilancia masiva de la *NSA* sabedores de que sus servicios de inteligencia nacional emplean métodos similares de cara a la prevención de amenazas, cuando no son cooperadores activos de la *NSA* en relación con alguno de sus programas. **La hipocresía internacional** se ha convertido en la respuesta recurrente, debido en gran parte a la posición de Estados Unidos en el mundo como aliado estratégico global o en otras palabras, como el *hegemón* internacional.[3]

6). Por último, la dialéctica entre democracia y seguridad. Resulta cierto que el coste de la seguridad ha de implicar un relativo sacrificio de libertades, sin embargo, las filtraciones en la historia del Gobierno norteamericano nos han enseñado que el equilibrio en **la balanza entre las variables de seguridad y las de democracia en muchas ocasiones se declina en favor de la primera: la seguridad.** Desde este punto de vista, se entiende que en un sistema democrático garantista, los ciudadanos deben tener garantizados derechos tales como, la privacidad o al honor, por encima de los intereses de seguridad. La conducta ejemplar de los ciudadanos nunca debe suponer la intromisión en su privacidad y no debe implicar un consentimiento implícito a la intromisión y vigilancia.

## 1.4. Marco teórico y aproximación conceptual.

La mayoría de estudios académicos sobre seguridad y su papel en las Relaciones Internacionales se desarrollaron en la etapa inmediata posterior a la Segunda Guerra Mundial. En general, se consideraban una subdisciplina de los estudios sobre Relaciones Internacionales, un campo de estudio dominado por el pensamiento anglo-estadounidense. Los es-

3 Se entiende por *hegemón* un Estado poderoso, capaz de instrumentalizar las relaciones internacionales con el único objetivo de conservar su poder en el ámbito internacional global y en detrimento de los demás actores internacionales.

tudios de seguridad se convirtieron en sinónimo de estudios estratégicos, manteniendo en sus formulaciones un inherente enfoque militar. Esta vertiente académica pronto impulsó en sus teorías la necesidad de protección del Estado mediante el desarrollo de una agenda que trabajara para asegurar el Estado-nación de presumibles amenazas y preservar así el *statu quo*.[4]

Casi la totalidad de los estudios de seguridad durante el desarrollo de la Guerra Fría reafirmaron una obviedad, la enorme influencia que han tenido los presupuestos ontológicos de realismo y neorrealismo en la investigación de la dinámica internacional.[5] No obstante, pronto comenzaron a emerger métodos alternativos de análisis sobre seguridad, uno de ellos el presentado por la Escuela de Copenhague entre las décadas de los 70 y 80.

La Escuela de Copenhague trató de responder a la preocupación tradicionalista de convertir todo en materia de seguridad a través de la definición del enfoque de seguridad. Para la Escuela este enfoque quedaba definido en primer lugar, por el desarrollo de la consideración de amenaza, ya no sólo vinculada a la dimensión militar, sino ampliando el campo de su estudio.[6]La Escuela formuló una comprensión teórica constructivista de la seguridad que le ha enfrentado con el tiempo a la visión objetivista tradicional de amenazas que sustenta la versión realista de la seguridad, pues para la Escuela, la "*realidad*" no es algo dado, por el contrario, es una construcción social.

Este método constructivista social de la conceptualización de seguridad conocido como "*Securitización*" se presentó por primera vez en un documento de trabajo de 1989: "*Security the Speech Act: Analysing the Politics of a Word*" por Ole Wæver. Para Weaver, esta Securitización es el establecimiento intersubjetivo de una amenaza existencial, lo que exige una atención urgente e inmediata, así como el uso de medidas extraordinarias para hacer frente a esta amenaza. En una definición de seguridad elaborada por la Escuela de Copenhague, se dice que esta consiste en librarse de las amenazas y ser capaz de mantener su independencia en lo que se refiere a su identidad y a su integración funcional frente a fuerzas de cambio consideradas hostiles.[7]

Según la Escuela de Copenhague, uno de los problemas fundamentales a la hora de abordar el concepto de seguridad es el objeto referente de seguridad. Para el realismo así como para el neorrealismo, el objeto referente de seguridad es la integridad territorial del Estado, pues es el Estado el encargado único de preservar los intereses estatales y con ellos, garantizar su supervivencia. Así, tal como indica Gabriel Antonio Orozco, el objetivo central de la política de seguridad de un Estado debe ser, para realistas y neorrealistas, "*disponer de todos los medios indispensables (normalmente militares), así como los recursos necesarios para preservar el interés de la nación, pues con ello se logra mantener la integridad y librar de amenazas a aquellos intereses prioritarios del Estado*".[8]Por su parte, el constructivismo ve al interés nacional como la expresión de la identidad de una sociedad. De este modo, el constructivismo considera que gracias a las relaciones de identidad de los elementos del sistema es posible crear un tipo

4 CHARRETT, Catherine: *A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security*, International Catalan Institute for Peace (ICIP), Working Papers, December 2009, p. 9.

5 Para el realismo, el objetivo principal de cada Estado es el de garantizar su propia seguridad. El realismo sostiene que buscando esta seguridad los Estados condicionarán las relaciones interestatales según su nivel de poder. Este nivel estará determinado por sus capacidades estatales, tanto económicas como militares.

6 Para la Escuela de Copenhague una amenaza a la seguridad no existe como un hecho, objetivamente hablando. La amenaza surge de un proceso intersubjetivo construido socialmente. La Escuela sostiene que no existen amenazas objetivas a la seguridad sino que éstas se construyen a partir de la visión subjetiva de los seres humanos. La amenaza deja de ser militar para adquirir así naturaleza social, medioambiental, política y económica.

7 BUZAN, Barry: "New Patterns of Global Security in the Twenty-First Century", *International Affairs*, Vol. 67, nº 3, July 1991, p. 432.

8 ANTONIO OROZCO, Gabriel: "El aporte de la Escuela de Copenhague a los estudios de seguridad", *Revista Fuerzas Armadas y Sociedad*, nº 1, 2000, pp: 145-146.

de seguridad colectiva[9] capaz de preservar los intereses de los actores internacionales.[10]

Los problemas de seguridad, por tanto, no pueden ser abordados desde una sola perspectiva. La seguridad se aplica a un campo de múltiples dimensiones para preservar a un individuo, una sociedad o un Estado. De este modo, es necesario entender hasta qué punto la necesidad de seguridad y la respuesta a las múltiples amenazas diluyen la convivencia democrática. Con las filtraciones desde los años de la Guerra Fría el seno de la Administración norteamericana y en especial, del ex analista de la *NSA*, Edward Snowden, se ha confirmado lo que Jack Balkin ya anunció en el año 2008, el establecimiento de un Estado de vigilancia autoritario.[11]Por contraposición a un tipo de Estado de vigilancia democrático, caracterizado por la limitación de los datos que recoge y el énfasis en la transparencia y en la destrucción de los datos recogidos; según Balkin, un Estado de vigilancia autoritario se identifica por desarrollar constantemente mecanismos para impedir que cualquier información sobre él mismo sea dada a conocer. Sus acciones y la información que recopila se mantienen en secreto.

En el caso de Estados Unidos, de acuerdo con los modelos aportados por Balkin, nos encontramos ante un modelo híbrido, pues en naturaleza se trata de un Estado de vigilancia democrático pero con tendencia al desarrollo de instrumentos y decisiones que oculten sus funciones de vigilancia. Esto se percibe en el contexto actual con la política de seguridad desarrollada por el Presidente Obama. La política de seguridad de Estados Unidos desde que Obama accediera a la presidencia, en enero de 2009, ha estado marcada por unos ejes estratégicos. Por un lado, centrar el esfuerzo en áreas prioritarias,[12]por ejemplo en la región de Asia-Pacífico, donde China constituye la principal preocupación de la política exterior norteamericana. En esta región, Estados Unidos practica una estrategia que combina el uso de los poderes diplomático y militar. Por otro lado, el impulso de la política de delegación de responsabilidad. Así, el continente africano es un ejemplo claro en el que Estados Unidos, debido a la preocupación por la inestabilidad en el Sahel y el Golfo de Guinea, que pueden convertirse en base de operaciones para Al-Qaeda, pretenden aplicar el procedimiento de dejar que sean otros quienes asuman el liderazgo en materia de seguridad.[13]

Y finalmente la multilateralidad. Obama ha mostrado en múltiples ocasiones su preferencia por la acción multilateral en lugar de la estrategia unilateral empleada por su antecesor. Esto tiene que ver con la naturaleza de muchas de las amenazas que enfrenta Estados Unidos, como puedan ser el terrorismo transnacional, ataques cibernéticos, proliferación de armas de destrucción masiva, etc; que no llevan aparejadas una respuesta únicamente de necesidad militar. No obstante, las revelaciones de Snowden han puesto de manifiesto un nuevo eje estratégico en la política de seguridad durante la Administración Obama y que resulta del todo continuista con la política de su antecesor: la instrumentalización de la inteligencia y la vigilancia masiva como méto-

9 Para Rafael Calduch, el concepto de seguridad colectiva es equivalente al de seguridad común que utiliza el Informe *Palme*, si bien este último enfatiza la importancia del desarme sobre el recurso a la fuerza como instrumento de sanción contra el país agresor.
Véase CALDUCH, Rafael: *Dinámica de la Sociedad Internacional*, Colección de información y comunicación, Madrid, Ed: Centro de Estudios Ramón Areces, 1993, p. 407.
10 MERCER, Jonathan: "Anarchy and Identity", *International Organization*, Vol. 49, nº 2, 1995, pp: 231-232.
11 Jack Balkin, profesor de derecho en la Universidad de Yale, elaboró un artículo académico en el año 2008 titulado: "The Constitution in the National Surveillance State". En él, Balkin identifica dos tipos de Estados de vigilancia y los contrapone. El primero es un estado de vigilancia autoritaria, mientras que el segundo es un estado de vigilancia democrática.

12 Este eje estratégico en la política de seguridad de Estados Unidos apareció por primera vez en el documento del Departamento de Defensa: "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense", de Enero de 2012. En él ya se reconocen a las regiones de Oriente Medio y el "pivote" Asia-Pacífico como las principales preocupaciones geográficas para la seguridad de Estados Unidos.
13 Mientras delegan en esos territorios la seguridad a Gobiernos autóctonos, se ve con buenos ojos el liderazgo en la región de terceros países. Este es el caso de Francia con la puesta en marcha de la "*Operación Serval*" en Mali.

do de anticipación a amenazas. La razón de Estado subyacente a toda actividad de inteligencia. Esto último es lo que dota de carácter híbrido al modelo de Estado de vigilancia norteamericano. De esta manera, se plantea así la dialéctica entre democracia y seguridad y hasta qué punto es necesario extender esta última sin coartar los principios fundamentales de la primera.

Tal como señala Robert Dahl, es importante entender que la democracia no es únicamente un procedimiento de Gobierno, pues "*dado que los derechos son elementos necesarios, la democracia es también intrínsecamente un sistema de derechos*".[14]Y estos derechos, que le son absolutamente inherentes, deben estar efectivamente a disposición de los ciudadanos. "*No basta con prometer derechos democráticos en textos escritos, en la Ley, o incluso en un documento constitucional. Los derechos deben hacerse verdaderamente efectivos y estar efectivamente a disposición de los ciudadanos en la práctica*".[15]

De esta manera, si la seguridad implica vulnerar o someter derechos de los ciudadanos, parece lógico que un sistema fundamentado en los derechos se vea continuamente violentado. Para Tim Berners-Lee, inventor de la *World Wide Web*, la vigilancia gubernamental en la red con el afán de responder a la necesidad de seguridad se ha constituido en "*intromisión en los derechos humanos básicos y amenaza a los fundamentos de una sociedad democrática*".[16]

El acceso a información privada de millones de ciudadanos no sólo abre una brecha en el debate sobre la necesidad de apuntalar la exigencia democrática, sino que, al mismo tiempo, obliga a plantearse si el avance tecnológico de los servicios de inteligencia permite a estos ser capaces de influir en la política, la economía o el avance militar de Gobiernos aliados, y determinar sus decisiones mediante operaciones de naturaleza encubierta.[17]

Es importante entender que los Estados democráticos, en general, tienden a separar los servicios dedicados a inteligencia doméstica de los dedicados a inteligencia extranjera. Esto es así por su diferente naturaleza y aún más por el hecho de que las normas y leyes se aplican a las operaciones de inteligencia de forma diferente en territorio nacional que en el extranjero. Por un lado, las funciones de la inteligencia doméstica, en general, son obtener, evaluar y correlacionar la inteligencia relevante para la seguridad interna. La seguridad interna tiene como objetivo la protección del Estado, el territorio y la sociedad contra los actos de terrorismo, espionaje, sabotaje, la subversión, el extremismo, el crimen organizado, la producción y el tráfico ilícito de narcóticos, etc. Por su parte, las funciones de la inteligencia extranjera, en general son obtener, evaluar y correlacionar la inteligencia relevante para la seguridad exterior y la capacidad de alerta temprana. La seguridad externa requiere del conocimiento de las amenazas, peligros y riesgos, así como de las oportunidades y probabi-

14 DAHL, A. Robert: *La Democracia*, Ed: Ariel Quintaesencia, ed. 2012, pp: 59-60.
15 Ibíd., p. 60.
16 HOPKINS, Nick: "Surveillance, democracy, transparency – a global view", October 10, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/oct/10/surveillance-global-view-debate

17 Existen diversas tipologías de acción encubierta: la acción política, la acción económica, la propaganda y las actividades paramilitares. La acción política es una categoría que involucra desde acciones de apoyo financiero a los grupos políticos a la creación de la insurgencia. Algunos ejemplos conocidos incluyen la financiación de las fuerzas leales al Sha de Irán en 1953 o el derrocamiento del Presidente Allende en Chile. La acción económica ha sido el tipo menos utilizado de la acción encubierta de la *CIA*. Por ejemplo, este tipo de acción se empleó contra el Gobierno de Allende en Chile en la década de 1970 mediante el fomento de las huelgas laborales y depreciando el precio mundial del cobre. En cuanto a la propaganda, se refiere a la difusión de la información con el fin de influir en la opinión pública. Como ejemplo, en Guatemala, en 1954, la *CIA* creó una emisora de radio que promocionaba al ejército revolucionario para derribar al Presidente comunista Jacob Arbenz. Por último, las actividades paramilitares es un tipo de acción encubierta que a menudo se superpone con las acciones políticas y generalmente consiste en asesinatos y apoyo a las operaciones de guerrilla, como en Vietnam, Indonesia, Nicaragua, Angola y más recientemente Afganistán e Irak.
Véase TARIF, Mathilde: "Legitimizing the use of covert action in the eyes of the American people", July 21, 2015, *Hestia Expertise*, en: http://hestia.hypotheses.org/462

lidad de agresiones. Se necesita así, información sobre las intenciones, las capacidades y las actividades de las potencias extranjeras, organizaciones, grupos o personas que representen una amenaza real o potencial para el Estado y sus intereses.[18]

Por esta razón, la inteligencia es un concepto polisémico y ya no sólo debe entenderse como una acción de recolección de información, sino también de conocimiento. La propia *Central Intelligence Agency* (*CIA*), define inteligencia como el elemento que faculta "*el conocimiento y la prospectiva de conocimiento, acerca del mundo que nos rodea, y como preludio en la toma de decisiones de los policy makers*".[19]Para Sherman Kent, ex trabajador de la *CIA* y uno de los pioneros en el impulso del análisis de inteligencia, es "*el conocimiento con el que los civiles y los militares, salvaguardan la seguridad nacional del Estado*".[20]

Las actividades de inteligencia se desarrollan en el seno del conocido como ciclo de inteligencia. Según José Antonio Sainz de la Peña, este ciclo es "*la secuencia de actividades por la que se obtienen informaciones, se las procesa para convertirlas en inteligencia y se pone ésta a disposición de los que la necesitan*".[21]El ciclo, por lo general, se clasifica en cuatro fases: dirección, obtención, elaboración y difusión. En la fase de dirección se determina la necesidad; en la obtención se procede a la explotación de todas las fuentes disponibles de información; en la elaboración la información se transforma en inteligencia, donde entra en juego un criterio de interpretación y de valoración; y finalmente, en la etapa de difusión la inteligencia es entregada, en tiempo oportuno y por los medios adecuados, únicamente a los que la han requerido al inicio del ciclo. Por su parte, los sistemas de obtención de inteligencia pueden clasificarse en diferentes tipos, los más relevantes son: *HUMINT* o Inteligencia clásica, obtenida por medios humanos. *IMINT* o Inteligencia de Imágenes obtenida por sensores diversos, fotográficos, térmicos, infrarrojos, radares etc. *SIGINT* o Inteligencia de Señales que engloba a *COMINT* y *ELINT*. *COMINT* o Inteligencia de Comunicaciones obtenida de escuchas o interceptaciones. *ELINT* o Inteligencia Electrónica obtenida de las radiaciones electromagnéticas, distintas de las usadas en transmisiones.[22]

La existencia de servicios de inteligencia en regímenes democráticos posibilita una paradoja política. Por un lado los servicios de inteligencia se establecen para proteger y garantizar la seguridad efectiva del Estado, sus ciudadanos y el orden democrático. Por otro lado, en virtud de sus funciones y capacidades en las diferentes etapas de su ciclo, disponen del potencial suficiente para socavar la garantía democrática de los ciudadanos, poner en peligro el Estado y subvertir el proceso democrático. En la actualidad, las democracias se enfrentan al reto de facilitar la convivencia efectiva entre los intereses de seguridad y la construcción de normas, controles y otras medidas de seguridad para proteger los derechos y libertades y prevenir los excesos de los servicios de inteligencia.

18 Geneva Centre for Democratic Control of Armed Forces: *Intelligence Services and Democracy*, Working paper series, nº 13, Switzerland, April 2002, en: http://www.ciaonet.org/attachments/9624/uploads

19 Central Intelligence Agency (Office of Public Affairs), *A Consumer's Guide to Intelligence*, Washington, DC: Central Intelligence Agency, 1999, p. 7.

20 KENT, Sherman: *Strategic Intelligence for American World Policy*, Ed. Princeton, NJ: Princeton University Press, 1949, p. 7.

21 SÁINZ DE LA PEÑA, José Antonio: "Inteligencia táctica". *Revista UNISCI*, nº 28, Enero 2012, ISSN 1696-2206, p. 222.

22 Ibíd., p. 224.

## *LISTA DE ACRÓNIMOS*

**ACLU**: American Civil Liberties Union. **AFSA**: Armed Forces Security Agency. **AFSC**: Afghanistan SIGINT Coalition. **BND**: Bundesnachrichtendienst.

**CIA**: Central Intelligence Agency.

**CJFE:** Canadian Journalists for Free Expression. **COINS**: Community On-line Information System. **COINTELPRO**: Counter Intelligence Program.

**COMINT**: Inteligencia de Comunicaciones.

**CNCI**: Comprehensive National Cybersecurity Initiative.

**CSS**: Central Security Service.

**CSEC**: Communications Security Establishment Canada.

**CSIS**: Center for Strategic and International Studies.

**DIA**: Defense Intelligence Agency. **DNI**: Digital Network Intelligence. **DNR**: Dialed Number Recognition. **DoD**: Departament of Defense.

**DOJ**: Department of Justice.

**DSD**: Defence Signals Directorate. **ELINT**: Inteligencia Electrónica. **FBI**: Federal Bureau of Investigation.

**FISA**: Foreign Intelligence Surveillance Act. **FISC**: Foreign Intelligence Surveillance Court. **GAO**: Global Access Operations.

**GCHQ**: Government Communications Headquarters.

**GCSB**: Government Communications Security Bureau.

**GTE**: Global Telecoms Exploitation.

**HRW**: Human Rights Watch.

**HUMINT**: Inteligencia Humana.

**IBM**: International Business Machines Corp.

**JCS**: Joint Chiefs of Staff.

**NCPC**: National Counterproliferation Center.

**NCTC**: National Counterterrorism Center.

**NME**: National Military Establishment. **NRO**: National Reconnaissance Office. **NSA**: National Security Agency.

**NSC**: National Security Council.

**ONU**: Organización de las Naciones Unidas.

**OSS**: Office of Strategic Services.

**OTAN**: North Atlantic Treaty Organization.

**PCLOB**: Privacy and Civil Liberties Oversight Board.

**PIPEDA**: Personal Information Protection and Electronic Documents Act.

**RCA:** Radio Corporation of America. **RMA**: Revolution in Military Affairs. **SIGINT**: Inteligencia de Señales.

**SSEUR**: SIGINT Seniors Europe. **SSO**: Special Source Operations. **SSPAC**: SIGINT Seniors Pacific.

**STANCIB**: State-Army-Navy Communication Intelligence Board.

**UCMJ**: The Uniform Code of Military Justice.

**USC**: United States Code.

**USCIB**: United States Communications Intelligence Board.

## 2. La construcción de la maquinaria de inteligencia norteamericana.

### 2.1. La National Security Act. Erigiendo la estructura de inteligencia. [1947]

El diseño de la estructura de inteligencia norteamericana como respuesta a los desafíos del panorama internacional comienza a trazarse en cursiva desde mediados del siglo XX. Ya durante la Segunda Guerra Mundial, la *Office of Strategic Services* (*OSS*), creada a propósito en 1942, aglutinó las tareas propias en clave de espionaje y contrainteligencia secreta frente a las potencias del eje.[1]En abril de 1945, Harry S. Truman asumió la presidencia a cuatro meses de confirmarse el fin de la contienda. La llegada de Truman a la Casa Blanca modificó el modelo de pensamiento de una inteligencia coyuntural, capaz de adaptarse a las amenazas, por una más pragmática, habilidosa y articulada, capaz de prevenirlas, todo ello en el marco de la confrontación bipolar con la Unión Soviética y con el incipiente halo de incertidumbre en torno al liderazgo mundial.

Producto de ello, Truman, con el respaldo del Congreso, llevó a cabo el 26 de julio de 1947, la firma de la *National Security Act*, el documento que dota de personalidad al aparato de inteligencia norteamericano. La intención del Congreso, tal como se especifica al comienzo de la Ley era *"proporcionar un programa integral para la seguridad futura de los Estados Unidos"*.[2]En definitiva, prever por un lado, un programa de inteligencia capaz de garantizar la seguridad nacional (como mecanismo de respuesta frente a la URSS) y, por otro, la dirección unificada bajo control civil de los Departamentos de las Fuerzas Armadas y sus tres Ejércitos, el de Tierra, Aire y Mar, pero bajo ningún concepto, fusionarlos. Esta reordenación se haría bajo mandato del *National Military Establishment* (*NME*)[3] a partir de ahora subordinado al Secretario de Defensa[4] y después de 1949, conocido como el nuevo *Department of Defense* (*DoD*).

La primera gran novedad de la Ley fue la creación de un *National Security Council* (*NSC*), el organismo encargado de asesorar al Presidente respecto a *"la integración de las políticas nacionales, exteriores y militares, relacionadas con la seguridad nacional"*.[5]Continuando el afán recopilador de los diferentes departamentos, la Ley incide en valorar y evaluar los objetivos, compromisos y riesgos de los Estados Unidos en aras de incrementar el interés en la seguridad nacional dado el contexto de confrontación bipolar y cuestionamiento del liderazgo global de Estados Unidos por parte de la URSS, especialmente tras la aplicación de la Doctrina Truman a partir de 1947.[6]

Tras la creación de un Consejo de Seguridad específico, la siguiente cuestión abierta era el acoplamiento en este nuevo escenario de la *OSS* operativa durante la Segunda Guerra Mundial.[7] De este

1 La *OSS* se dividía en varias secciones especializadas: *Research and Analysis (R&A), Secret Intelligence (SI), Special Operations (SO), Moral Operations (MO), Operational Groups (OG), Maritime Unit (MU)* y el departamento de contraespionaje *(X-2),* que se encargaba de garantizar el éxito de las operaciones aliadas tratando de evitar las infiltraciones enemigas.

2 Public Law 253-80th Congress: *The National Security Act of 1947*, "*Declaration of Policy*", Chapter 343, 1st Session; S. 758, July 26, 1947, p. 2, en: https://assets.documentcloud.org/documents/2695389/1947-National- Security-Act.pdf

3 *El Establishment militar nacional estará integrado por los Departamentos de la Armada, de la Marina y de la Fuerza Aérea junto con todos los demás organismos creados bajo el título II de esta Ley.*
Ibíd., Title II: The National Military Establishment, Sec. 201: "Establishment of the National Military Establishment".

4 La mayoría de las reglamentaciones del acta tomaron efecto el 18 de septiembre de 1947, un día después de que el Senado confirmara a James V. Forrestal como el primer Secretario de Defensa.

5 Public Law 253: *The National Security Act*, op. cit., Title I: Coordination for National Security, Sec. 101: "National Security Council".

6 Lo que el Presidente Truman enunció ante el Congreso como una proclama por la persistencia de los pueblos libres frente a presiones exteriores acabó por convertirse en medida de contención del comunismo en la Europa oriental. El plan concedió 400 millones de dólares en ayuda económica y militar para Turquía y Grecia, enclave donde transcurría por entonces la Guerra Civil (1946-1949).

7 El 20 de septiembre de 1945 el Presidente Truman firma la Orden Ejecutiva *9621* por medio de la cual se produce la disolución definitiva de la *OSS*.

modo, la *National Security Act* de 1947 reestructura el espacio dejado por la *OSS* y le confiere rango departamental, dando lugar así a la *Central Intelligence Agency* (*CIA*)[8]por vez primera y enumera sus funciones bajo coordinación del Consejo. Entre ellas, se encuentran el asesoramiento al Consejo, la correlación y evaluación de la inteligencia filtrada al Consejo o las meras recomendaciones al mismo cuando la seguridad nacional se vea involucrada, así como las labores de interconexión entre los diferentes departamentos.

La Guerra Fría se convirtió así, en el escenario perfecto para legitimar una estructura de seguridad nacional moderna donde los nuevos departamentos emergentes como el de Defensa, la *CIA* o el propio *NSC*, multiplicaron muy pronto su protagonismo, siempre bajo el auspicio de la *National Security Act*.[9]

Otra gran aportación de la *National Security Act* fue la creación específica del cargo de Secretario de Defensa,[10] al que el documento se refiere como *"el segundo en la cadena de mando al Presidente en todos los asuntos relacionados con la seguridad nacional,"*[11] a diferencia de los Jefes de Estado Mayor, también figuras relevantes erigidas en esta Ley y definidos como *"los principales asesores militares al Presidente y el Secretario de Defensa"*.[12]

Entre las tareas del reciente Secretario de Defensa se encuentran el establecer políticas y programas para el *Establishment* militar y todos los departamentos, desde las Fuerzas de Tierra a las Aéreas y Marítimas, pasando incluso por el *Joint Chiefs of Staff* (*JCS*) o la *Munitions Board*. No obstante, habría de esperar hasta el 10 de agosto de 1949, cuando por enmienda a la Ley, la *National Security Act* original concibiera la dependencia de cada uno de los respectivos secretarios de los Departamentos de la Fuerzas Armadas al Secretario de Defensa dotándole así de una mayor autoridad en la nueva comunidad de inteligencia norteamericana,[13]todo ello al frente del nombrado, desde esta fecha, *Departament of Defense*. Con esta ligera modificación, el Secretario de Defensa pasaba de ser un mero asesor principal al segundo eslabón de mando en la cadena militar.[14]

Desde la perspectiva departamental, la Ley resulta de gran aprovechamiento si atendemos a los cambios organizativos. El cambio de denominación del Departamento de Guerra (más propio de épocas pasadas) al de Ejército, la pertenencia de las distintas fuerzas al *Establishment* militar nacional creado bajo liderazgo del Secretario de Defensa o la creación de los ya nombrados Jefes de Estado Mayor, entre cuyas funciones se enumeran la preparación de planes logísticos y estratégicos y la formulación de políticas para prever la dirección de las fuerzas militares, son sólo algunas de las contribuciones de la Ley.

---

8 *Con un Director que será la cabeza de la misma. El Director será nombrado por el Presidente, por y con el consejo y consentimiento del Senado, de entre los funcionarios encargados de las fuerzas armadas o de entre individuos en la vida civil. El Director deberá recibir una compensación a razón de 14.000 dólares al año.*
Ibíd., Sec. 102: "Central Intelligence Agency".

9 Tal como indica Cambone, la Guerra Fría dio lugar a un enorme incremento en el tamaño de las Agencias gubernamentales comprometidas con el avance de la misma. Pero lo que nos interesa aquí no es tanto el tamaño al que el Gobierno y sus departamentos crecieron, sino la tendencia de las organizaciones gubernamentales en enfatizar la aplicación constante y económica de las capacidades de Estados Unidos en la persecución de los objetivos de la Guerra Fría.
Véase CAMBONE, A. Stephen: *A New Structure for National Security Policy Planning*, Ed: Center for Strategic & International Studies, 1998, p. 44.

10 Antes de su creación específica lo que existía era el propio *National Military Establishment*, creado en esta misma Ley como un comando militar unificado.

11 Public Law 253: *The National Security Act*, op. cit., Title II: The National Military Establishment, Sec. 202: "Secretary of Defense".

12 Ibíd., Sec. 211: "Joint Chiefs of Staff".

13 *El Departamento de la Armada, el Departamento de la Marina y el Departamento de la Fuerza Aérea, deberán ser administrados como Departamentos ejecutivos individuales por sus respectivos secretarios, cuyos poderes quedarán sujetos y conferidos al Secretario de Defensa.*
Véase Public Law 216-81st Congress*: The National Security Act of 1947 as amended by Public Law 216*, approved August 10, 1949, Title II: Department of Defense, Sec. 202: "Secretary of Defense", en: http://history.defense.gov/Portals/70/Documents/dod_reforms/NSA1947amended1949.pdf

14 Cambone, *A New Structure*, op. cit., pp: 43-44.
Fuente: *Department of Defense* (*DoD*). [1949-1950]

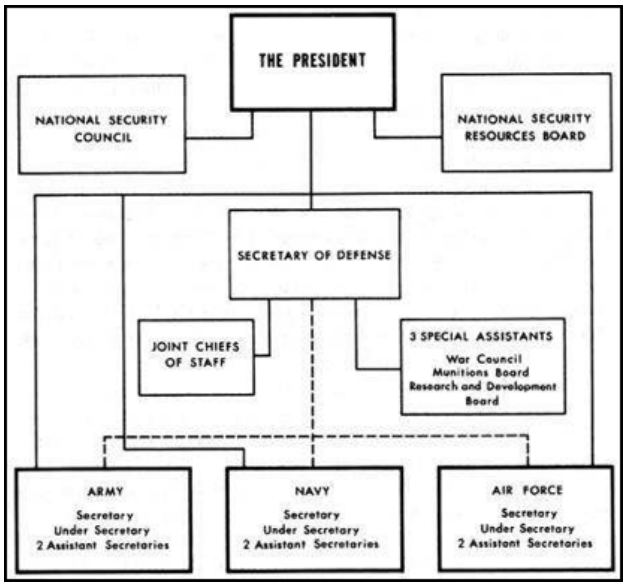
Si atendemos a la organización de la comunidad de inteligencia después de la enmienda de 1949 a la *National Security Act*, lo que se observa es la dependencia inmediata al Presidente, del recién creado *NSC*; así como el protagonismo adquirido en la cadena de mando por el Secretario de Defensa debido a la construcción del propio *DoD* en lugar del *National Military Establishment*, que coordinaba las funciones de las diferentes áreas antes de 1949.

## 2.2. De la Armed Forces Security Agency a la National Security Agency. [1949-1952]

El predecesor de la *National Security Agency* (*NSA*), la *Armed Forces Security Agency* (*AFSA*), se creó dentro del marco de dependencia del reciente *DoD*[15] el 20 de mayo de 1949. Según indica Thomas L. Burns, la misión de *AFSA* era "*llevar a cabo todas las actividades de seguridad de inteligencia y comunicaciones dentro del Departamento de Defensa, excepto las realizadas por los servicios militares*".[16]

No obstante, la historia de *AFSA* resulta breve. Las dos grandes razones que explican su fracaso fueron: su intento de centralizar el esfuerzo de las actividades de *COMINT* (Inteligencia de Comunicaciones tales como el teléfono o la radio) lo que hizo emerger un cierto recelo en las Agencias encargadas para tal fin con anterioridad, como la *CIA* y el *Federal Bureau of Investigation* (*FBI*), y a la vez, que el Director de la *AFSA* no tuviera la autoridad[17] directa sobre los diferentes servicios militares norteamericanos. La falta de eficiencia se puso de manifiesto con especial hincapié en la guerra de Corea iniciada en junio de 1950 (1950-1953).

Por esta razón, en diciembre de 1951, el Presidente Truman decidió emplear todas sus fuerzas en renovar el aparato interno de inteligencia toda




Fuente: Department of Defense (DoD). [1949-1950]

vez que la legislación desde la *National Security Act* de 1947 ya había proferido la estructura. Entre sus solicitudes en un primer memorando se recogió el intento de crear una Junta de Inteligencia y constituir un Comité[18] que marcará los primeros pasos de lo que desde entonces se conocerá como la *National Security Agency*.[19]

El *Brownell Committee*,[20] iniciado el 28 de diciembre de 1951, concluyó en su informe en la necesidad de sacrificar la *AFSA* y se erigió en una

15 Dirigido por Louis A. Johnson en este momento.
16 BURNS, L. Thomas: *The Origins of the National Security Agency 1940-52*, Center for Cryptologic History, U.S. National Security Agency (*NSA*), Chapter IV: Creation of the Armed Forces Security Agency, Series V: Volume I, 1990, p. 59.
17 Ibíd.

18 Truman estableció el Comité para llevar a cabo una investigación sobre la eficiencia y la organización de todo el esfuerzo de Inteligencia de Comunicaciones estadounidense. Para diciembre de 1951, el decepcionante rendimiento de la *AFSA* en tiempo de guerra había señalado a la Casa Blanca la necesidad de una revisión completa de la estructura de *COMINT*.
Ibíd., p. 99.
19 El memorando del Presidente contenía la primera referencia a una "National Security Agency", que se establecerá en el lugar de la *Armed Forces Security Agency*. En virtud del memorando, el Departamento de Defensa se convertiría en el agente ejecutivo del Gobierno para la producción de información de Inteligencia de Comunicaciones eliminando de este modo a la *Joint Chiefs of Staff* como autoridad de control para el proceso de *COMINT*.
Ibíd., p. 97.
20 El 13 de diciembre de 1951 el Presidente Truman ordenó la puesta en marcha oficial del Comité, configurado por los Secretarios de Estado y de Defensa en colaboración con el Director de la *CIA*. El Comité dio comienzo el 28 del mismo mes y fue presidido por George Brownell, un eminente abogado de Nueva York.

especie de Carta Magna en la coordinación y trabajo de las tareas de *COMINT*[21] en manos de la *NSA* destacando la necesidad de involucrar al aparato militar dentro de la Agencia para no cometer errores del pasado. Como respuesta al informe Brownell, Truman, el 24 de octubre de 1952 elaboró un segundo memorando[22] que procedió al asentamiento del nuevo organismo de inteligencia y ejecutó reformas estructurales.

Así, conociendo las recomendaciones del Comité, en diciembre de 1952, el *NSC* con el objetivo de legitimar los cambios que se llevaron a cabo impulsados desde la presidencia, reformó la redacción de la Directiva nº 9: *Communications Intelligence* del 10 de marzo de 1950,[23]por medio de la cual se recogieron y enumeraron las misiones de la *NSA* así como de su Director. Con el remozado de su escrito, este es el primer documento en el que aparecen redactadas las funciones de la Agencia y de sus órganos decisorios.

La misión de la *NSA*, en lo que respecta a las funciones de *COMINT*, se reduce a la protección y el control eficaz de la Inteligencia de Comunicaciones de los Estados Unidos frente a Gobiernos extranjeros. Del mismo modo, se especifica que el Director de la *NSA* debe desarrollar su capacidad técnica siempre bajo coordinación del Secretario de Defensa y de acuerdo a las políticas aprobadas por la *United States Communications Intelligence Board* (*USCIB*),[24] conformada por: el Director Central de Inteligencia, un representante del Secretario de Defensa, un representante del Secretario de Estado, un representante del *FBI*, el propio Director de la *NSA*, un representante de cada Departamento de las Fuerzas Armadas: Tierra, Aire y Marina y por último, un representante de la *CIA*.

Finalmente, también se recogen los requisitos para ostentar el cargo de Director de la Agencia: ser designado por el Secretario de Defensa, ocupar el cargo un mínimo de cuatro años y ser oficial de carrera encargado de las Fuerzas Armadas en activo o reactivado y que goce al menos de un rango de 3 estrellas. Entre sus funciones se encuentran desde la formulación de los planes operativos para la coordinación de las tareas de *COMINT*, así como emplear el capital humano a su alcance para lograr la mayor eficiencia. De esta manera, la *NSA* echaba a andar.

## 3. La National Security Agency: Etapas en la configuración del centinela global.

### 3.1. La NSA en la Guerra Fría. [1952-1991]

#### 3.1.1. El antecedente de la vigilancia: El Counter Intelligence Program. [1956-1971]

En plena escalada de la Guerra Fría y tras la consecución de una comunidad primigenia de inteligencia sostenida por el *NSC*, el *FBI* inició en 1956 un conjunto de operaciones de contrainteligencia bajo la denominación del *Counter Intelligence Program* (*COINTELPRO*). El propósito, tal como indican Ward Churchill y Jim Vander Wall, no era otro que "*perturbar, desestabilizar, paralizar, destruir o*

21 El informe final recomendó una reorganización completa en las tareas de *COMINT* y proporcionó un modelo para la nueva estructura. Del mismo modo, el Comité Brownell presionó para que la Inteligencia de Comunicaciones adquiriese un nuevo estatus de atención e interés a nivel nacional.
Véase Burns, *The Origins of the*, op. cit., p. 97.

22 TRUMAN, S. Harry: *Memorandum from President Harry S. Truman to the Secretary of State*, the Secretary of Defense, Subject: Communications Intelligence Activities, 24 October 1952, en: https://www.nsa.gov/public_info/_files/truman/truman_memo.pdf

23 National Security Council Intelligence: *Directive nº 9. Communications Intelligence,* 10 March 1950, en: http://fas.org/irp/offdocs/nscid09.htm

24 Además, en la Directiva se especifica que solo a los departamentos o Agencias que están representadas en la *USCIB*, se les autoriza a participar activamente en actividades de *COMINT*.
Véase National Security Council Intelligence reform: *Directive nº 9. Communications Intelligence*, 29 December 1952, en: http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa02b.pdf

*de otra manera, neutralizar, los individuos y grupos políticos disidentes en los Estados Unidos*".[25]

Las operaciones de vigilancia del *FBI*, dentro de sus competencias en materia de seguridad interior, y que pueden ser consideradas como una antesala a la vigilancia del siglo XXI, reflejaban los traumas derivados de la confrontación bipolar y el cuestionamiento del liderazgo global, encontrando en el *Macarthismo* (entre 1950 y 1956) y el panóptico obsesivo de J. Edgar Hoover al frente de la Oficina, los perfectos aliados para la desaparición de cualquier tipo de disidencia. Los principales puntos de interés los concentraba el Partido Comunista, al que se asociaba a una entidad criminal y se orientaban la mayor parte de las acciones desarrolladas en el marco de *COINTELPRO*, como deja constancia en una misiva el propio Hoover el 28 de agosto de 1956 incentivando al sabotaje potencial.[26]

A pesar de configurarse como el bastión anticomunista, las prácticas de *COINTELPRO* se extendieron de igual manera a los grupos pro derechos civiles, especialmente el Movimiento de Liberación Negro o el Movimiento por la Independencia de Puerto Rico. En el primer caso, el desgaste hizo desaparecer al Partido de las Panteras Negras,[27]como referente de la Liberación, a pesar de que hacia 1974 todavía persistiera una filial en Oakland. En el caso del movimiento independentista puertorriqueño, la desinformación y la cooperación con los medios de comunicación fue la carta que hizo valer la Oficina para desacreditar la tendencia comunista del mismo.

De acuerdo a las líneas oficiales de investigación, *COINTELPRO* tuvo una vigencia de quince años, entre 1956 y 1971. Durante este tiempo, el *FBI* admitió haber participado en 2.218 operaciones junto con otro tipo de prácticas, hoy más frecuentes, como la escucha telefónica sin orden judicial y la interceptación de la correspondencia con la colaboración de la *CIA*.[28]

Según Glenn Greenwald, Cuando el contraespionaje interno del *FBI* salió a la luz en 1971, el escándalo público, acrecentado con las pesquisas de Nixon en el caso *Watergate* (1972), iniciaron inevitablemente la conformación del *Church Committee*, y aceleraron la conclusión de que durante quince años el *FBI* llevó a cabo una sofisticada operación de vigilancia dirigida de lleno a impedir el ejercicio de las libertades de expresión y de prensa de la Primera Enmienda.[29]

La investigación de Frank Church puso de manifiesto el etiquetado político de medio millón de ciudadanos norteamericanos como subversivos potenciales, aunque como indica Greenwald, no fueron los únicos abusos de vigilancia descubiertos por el Comité.[30]

25 CHURCHILL, Ward & VANDER WALL, Jim: *The COINTELPRO Papers. Documents from the FBI's Secret Wars against Domestic Dissent*, Boston, Ed: South End Press, 1990, Preface, p. 10.

26 La carta, dirigida a funcionarios que desempeñaban labores de contrainteligencia en el *FBI*, instaba a crear "programas de acción" destinados a la negación absoluta del Partido Comunista. Programas capaces de influir en las masas y de moldear a la opinión pública.
Ibíd., p. 33

27 Se trataba de un partido establecido originalmente en el área de la bahía de San Francisco por los estudiantes universitarios Merritt Huey P. Newton y Bobby Seale en octubre de 1966. En el otoño de 1968, el *FBI* consideró que el Partido de las Panteras Negras era una organización catalizadora de un movimiento de liberación negro. El 8 de septiembre de 1968 en una entrevista concedida a *The New York Times*, J. Edgar Hoover dejó constancia de que el Partido de las Panteras constituía "la amenaza más grande para la seguridad interior del país".
Ibíd., p. 123.

28 Las escuchas telefónicas sin orden judicial alcanzaron el total (que se tenga constancia) de 2.305, mientras que la interceptación de la correspondencia confidencial por la *CIA*, en su trabajo complementario con el *FBI*, alcanzó los 57.846 casos.
Ibíd., p. 303.

29 Basándose en la teoría de que, al obstaculizar el desarrollo de grupos peligrosos y la propagación de ideas peligrosas, se protegía la seguridad nacional y se prevenía la violencia.
Véase GREENWALD, Glenn: *Snowden: Sin un lugar donde esconderse*, Ediciones B, 2014, p. 229.

30 En su informe final declaraba que de 1947 a 1975, la *NSA* obtuvo millones de telegramas privados enviados desde, a, o a través de Estados Unidos en virtud de un acuerdo

### 3.1.2. La National Reconnaissance Office (NRO). Comienzo de las rivalidades entre Agencias Ejecutivas de vigilancia. [1961]

A finales de la década de los cincuenta se produjo un definitivo paso hacia delante de las tecnologías relacionadas con el desarrollo de cohetes y sensores nucleares[31] que sin duda, ayudaron a Estados Unidos a la hora de enfrentar el problema más amenazante de seguridad nacional: la forma de analizar las fuerzas militares soviéticas y evitar una potencial guerra nuclear empleando para ello la política de disuasión.

Casi veinte años después del ataque japonés a Pearl Harbor, el Director de la *CIA*, el general Charles Cabell, estableció el 6 de septiembre de 1961[32] el memorándum Roswell Gilpatric,[33] por el que nació la *National Reconnaissance Office* (*NRO*), en un afán de despejar los fantasmas del pasado y con la esperanza de que, por medio de tecnología satelital y la agrupación de un equipo de científicos de gran formación,[34] Estados Unidos nunca tendría que volver a enfrentarse a sorpresas tan devastadoras. Esta tecnología de reconocimiento comprendía desde sus orígenes, ambiciosos planes de seguridad nacional estrechamente ligados a la acción militar de la *CIA* o a los primeros programas desarrollados en el seno de la *NSA*. Aunque su principal protagonismo lo adquirirá al ser capaz, no sólo de lanzar al espacio satélites de forma periódica, y hacerlo sin fallo, sino una vez en él, poder enviar gradualmente información en forma de fotos.[35]La *NRO*, a pesar de experimentar fracasos, que en la mayoría de los casos encontraban el respaldo y el liderazgo del Presidente Eisenhower, pronto comenzó a dar respuesta exitosa[36] a la amenaza soviética.

---

secreto con tres empresas de telégrafos del país. Por otra parte, durante una operación de la *CIA*, *CHAOS* (1967-1973), unos 300.000 individuos fueron clasificados en un sistema informático de la *CIA*, y se crearon expedientes separados sobre aproximadamente 7.200 norteamericanos y más de 100 grupos nacionales. Además, se calcula que había unos 100.000 norteamericanos incluidos en los expedientes de inteligencia del Ejército de Estados Unidos elaborados entre mediados de la década de 1960 y 1971 al tiempo que unos 11.000 individuos eran investigados por el servicio de Impuestos Internos basándose en criterios más políticos que fiscales.
Ibíd., p. 230.

31 Ya durante la Segunda Guerra Mundial se había dado el pistoletazo de salida a la tecnología nuclear. Alemania inició el Proyecto Uranio y la URSS la Operación Borodino. No obstante, sería Estados Unidos el primer país en disponer de la Bomba nuclear y por ende, de toda su tecnología, gracias al desarrollo del Proyecto Manhattan con ayuda parcial del Reino Unido y Canadá. El primer ensayo con éxito tiene lugar en Nuevo México el 16 de julio de 1945. Utilizando los datos exitosos de este primer test, los soviéticos dispondrán de la bomba a partir del ensayo realizado en Semipalatinsk, el 22 de agosto de 1949.

32 Tal como señala Gustavo Díaz Matey, cuando John F. Kennedy llegó a la presidencia de EEUU en 1961, su secretario de Estado, Robert McNamara, añadió otra pieza a la comunidad de inteligencia con la creación de la *DIA*, la Agencia de Inteligencia de Defensa, cuya misión es consolidar la producción de inteligencia por parte de los militares ayudando al secretario de Defensa y el *JCS*.
Véase DÍAZ MATEY, Gustavo: "La comunidad de inteligencia estadounidense tras las elecciones de noviembre de 2008: retos y oportunidades de la Administración Obama", *Real Instituto Elcano*, Documento de Trabajo nº 6, 5 Febrero, 2009, p. 6

33 Subsecretario de Defensa en el intervalo 1961-64, jugó un papel fundamental en las estrategias de seguridad nacional frente a la ubicación soviética de misiles en Bahía de cochinos, asesorando tanto al Presidente Kennedy, como al Secretario de Defensa, Robert McNamara.

34 Un grupo de gran talento de individuos de diversos orígenes jugó un papel importante en la *NRO*. Estos individuos fueron sobre todo, el Dr. James Killian, asesor científico del Presidente Eisenhower y Presidente del Instituto de Tecnología de Massachusetts, que proporcionó un apoyo fundamental para los sistemas nacionales de reconocimiento. El Dr. Edwin Land, inventor de la fotografía instantánea y el Presidente de la Polaroid Corporation, que se convirtió en un defensor acérrimo del empleo de las nuevas tecnologías para resolver los problemas de inteligencia. Y por último, el Dr. Richard Bissell, desarrollador de dos programas de éxito: el avión espía *U-2* y el primer programa de reconocimiento fotográfico satélitel, *CORONA*.
Véase BERKOWITZ, Bruce: *The National Reconnaissance Office at 50 years: A brief history*, Center for the Study of National Reconnaissance, National Reconnaissance Office, Chantilly, Virginia, Ed: Government Printing Office, September 2011, p. 5.

35 Los primeros satélites con la tecnología capaz de realizar fotografías del terreno fueron producidos y financiados por el *Directorate of Science & Technology* y la *CIA*. El programa adquirió el nombre en cave de *CORONA* y su papel fue clave en la defensa estratégica, el espionaje y la vigilancia de la URSS y la R.P. de China en el período de junio de 1959 a mayo de 1972.

36 El *U-2*, primer avión de gran altitud de la nación (capaz de volar a 70.000 pies de altura); *Grab*, el primer sistema de inteligencia de señales; y *CORONA*, ejemplifican la respuesta exitosa a los desafíos de la Guerra Fría en

Sin embargo, la constitución de la *NRO*, también trajo consigo fricciones internas entre Agencias. Desde que en septiembre de 1961 comenzara su operatividad, la *NRO*, para conseguir resultados eficaces, colaboraba con la *CIA* y el Departamento de la Fuerza Aérea. A pesar de que en el acuerdo de cooperación triangular, estos dos últimos no se veían obligados a ceder el control sobre cualquiera de sus programas de satélites de reconocimiento a la *NRO*, en noviembre de 1962, funcionarios del Departamento de la Fuerza Aérea propusieron la transferencia de estos programas de la *CIA* al departamento, hecho que contrastaba con la solicitud de la *CIA* de suprimir la *NRO*, al mismo tiempo que las diferencias entre la *NRO* y la *NSA* comenzaban a emerger por razón del coste de los sistemas de vigilancia espacial desarrollados.

### 3.1.3. Creación del Central Security Service. El complemento funcional de la NSA. [1972]

La década de los sesenta aumentó el espectro de aplicación de las tareas de la *NSA* debido a la absorción de las funciones de la *AFSA*, hecho que había permitido involucrar todas las áreas militares con plena participación y cesión de documentación clave en las funciones de inteligencia. No obstante, comenzada la década de los setenta y por Directiva del *DoD* se decide la creación en diciembre de 1971 (aunque entra en vigor en enero de 1972) del *Central Security Service* (*CSS*), un organismo como señala Keith P. Clive, pensado para promover la colaboración y combinación entre la *NSA* y los órganos de inteligencia de las Fuerzas Armadas especializadas en procedimientos criptográficos, y reforzado bajo la dirección de la misma persona para ambas Agencias.[37]

En la Directiva de 1971 se detalla con claridad el papel de la *NSA* como organización encargada de las tareas de Señales de Inteligencia (*SIGINT*) y del propio *CSS* como herramienta de soporte.[38] Del mismo modo, se reconoce en el documento el intento de dejar definitivamente incorporado en las tareas de vigilancia de la *NSA* a los diferentes estamentos militares, quienes desde la época de la *AFSA* habían sido reacios a colaborar con las Agencias de inteligencia. Para ello, el *CSS* daría cabida en su estructura a todos los cuerpos militares[39] estadounidenses, pero siempre bajo la dirección del Director de la *NSA*.

No obstante, la articulación del *CSS* como baza fortalecedora interna de la *NSA* contrastaba en este momento con las dudas alrededor de la Agencia, y que pusieron en peligro su supervivencia con motivo del *Church Committee* iniciado en 1974.

### 3.1.4. El Church Committee: Las revelaciones de los programas MINARET y SHAMROCK y las Watch Lists. [1974-1976]

Después de que *COINTELPRO* iniciara una década convulsa para la inteligencia norteamericana, la investigación del Comité del Senado iniciada en 1973 sobre el escándalo *Watergate* reveló que el Ejecutivo había dirigido la inteligencia nacional para llevar a cabo operaciones de espionaje constitucionalmente cuestionables.

Los intentos de espiar e intervenir las comunicaciones del Partido Demócrata que dinamitaron la carrera de Nixon como Presidente, no constituyen una novedad en absoluto en el proceder de la inteligencia norteamericana, como indicó el informe Church. Ya antes de la formulación de la *National*

este período.
Berkowitz, *The National Reconnaissance Office*, op. cit., p. 6.

37 CLIVE, P. Keith: "NSA´s Central Security Service", *U.S. Military Academy´s Cryptologia*, 2002.

38 Department of Defense Directive: *Directive nº 6. The National Security Agency and the Central Security Service*, December 23, 1971, Title II: Concept, p. 1, en: http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa07.pdf

39 El *CSS* estará integrado por: "un Jefe del propio CSS que lo será al mismo tiempo de la NSA, un Jefe adjunto, un cuartel general, los Departamentos del Ejército, la Armada, la Fuerza Aérea y la Marina, así como los demás integrantes o subordinados que le asigne a su servicio el Secretario de Defensa".
Ibíd., Title V: Organization and Resources, pp: 3-5.

*Security Act* de 1947, y a pesar de no contar con el respaldo estatutario necesario para hacerlo, los Presidentes tomaban las decisiones de inteligencia extranjera por su propia cuenta.[40]

El 21 de enero de 1975, el senador John Pastore presentó la Resolución donde se conformaba este Comité especial,[41]bajo presidencia de Frank Church (senador demócrata por Idaho) y con John Tower como Vicepresidente (senador republicano por Texas). Concebido para durar doce meses, aunque se prologara hasta los dieciséis, contrató alrededor de 150 funcionarios peinando más de 100.000 documentos clasificados y no clasificados y entrevistó a 800 personas, incluidos exdirectores de la *CIA*.[42] [42]Los investigadores concluyeron que desde la Administración del Presidente Franklin D. Roosevelt y hasta la década de los setenta, los excesos de vigilancia tanto dentro como fuera de las fronteras estadounidenses, se debían al ascenso norteamericano en el ejercicio de una superpotencia en plena confrontación bipolar, en el contexto de la Guerra Fría.[43]

Más allá de la vigilancia, el *Church Committee* también destacó en su informe final la falta de ensamblaje y coordinación entre el *FBI* y la *CIA* desacreditando por tanto el papel del llamado Plan Huston,[44]surgido a petición de Nixon con la premisa de aumentar la colaboración entre Agencias para la recopilación de información en suelo nacional.

Del mismo modo, el Comité, a pesar de las críticas permanentes recibidas desde el seno de la comunidad de inteligencia, por lo que se consideraba como una supervisión excesiva, concluyó en la necesidad de crear en abril de 1976, mediante la Resolución *400*, el Comité de Inteligencia del Senado,[45]y sentó las bases para la aprobación de la futura *Foreign Intelligence Surveillance Act* (*FISA*) ratificada en 1978, y firmada por el Presidente Jimmy Carter.

Durante las audiencias del Comité que supuso una supervisión y evaluación total de la comunidad de inteligencia, la *NSA* adquirió pleno protagonismo por la revelación a lo largo de las investigaciones de hasta dos programas desarrollados por la Agencia de cara a la interceptación masiva: *MINARET* y *SHAMROCK*, que permitió en colaboración con la *CIA*[46] la obtención de millones de telegramas priva-

40 Antes de 1947, el Congreso, a pesar de su considerable autoridad en los asuntos exteriores y de la defensa nacional, no legislaba directamente con respecto a la actividad de inteligencia exterior. En virtud de la cláusula necesaria y su poder para llevar a cabo las diversas regulaciones, el Congreso podría haber elaborado Leyes específicas para regular la conducta de inteligencia extranjera. En ausencia de tales estatutos o cláusulas, los Presidentes llevaron a cabo actividades de inteligencia extranjera antes de la *National Security Act* de 1947, utilizando para ello su propia autoridad.
Select Committee to Study Governmental Operations: *Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, United States: Congress, Library of Congress, Washington, April 29, 1976, p. 33, en: https://archive.org/details/finalreportofsel06unit

41 *Con objeto de investigar las operaciones de inteligencia federales y determinar en qué medida, en su caso, Agencias del Gobierno federal han llevado a cabo actividades ilegales, impropias o no éticas.*
United States Senate: *Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, (The Church Committee), Resolution passed January 27, 1975; Final Report issued: April 29, 1976, en: http://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm

42 United States Senate: *Church Committee Created*, January 27, 1975, en: http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm

43 *Los excesos de la Inteligencia estadounidense, tanto en el país como en el extranjero, no han sido producto de un Partido político o una Administración presidencial o un solo hombre, sino la consecuencia de que la nación se haya convertido en superpotencia en el transcurso de la Guerra Fría global.*
Ibíd.

44 Resultado de un informe de 43 páginas presentado por el ayudante del Presidente Nixon, Tom Charles Huston, en 1970. A mediados de julio del mismo año, Nixon ratifica las propuestas y lo presenta como documento de coordinación entre Agencias, a los Directores de la *CIA*, *FBI*, *DIA* y *NSA*.

45 Para proporcionar una "supervisión legislativa sobre las actividades de inteligencia de los Estados Unidos y asegurar que estas se desarrollan en conformidad con la Constitución y las Leyes de los Estados Unidos".
United States Senate, *Select Committee to Study Governmental Operations*, op. cit.

46 En la *Rockefeller Commission* de 1975, celebrada para evaluar y someter a análisis las actividades de la *CIA*, se indicó la cobertura que esta última habría proporcionado a

dos, así como las conocidas como listas de vigilancia (*Watch Lists*) que contenían multitud de nombres de ciudadanos estadounidenses objeto de vigilancia gubernamental.

En 1969, la *NSA* formalizó el programa *MINARET*, con el que daba comienzo a la elaboración de las listas de vigilancia. El proyecto fue el resultado de una campaña iniciada en el otoño de 1967, cuando se creó la *Civil Disturbance Unit*.[47]El programa no sólo se aplicaba, según reconocía el informe del *Church Committee*, a la influencia extranjera sobre la disidencia interna, sino también a los "*grupos e individuos americanos cuyas actividades podían dar lugar a disturbios civiles u otra manera de subvertir la seguridad nacional de los Estados Unidos*".[48]

Al mismo tiempo, es sus tareas, el propio proyecto se desmarcaba en su responsabilidad de la pertenencia a la organización, algo que dejó de ser así a partir de 1973, cuando el entonces Director de la *NSA*, el General Lew Allen, Jr.[49]suspendió el programa y reconoció la autoría de la Agencia detrás de las listas.

Por su parte, *SHAMROCK* era el nombre en clave del programa especial por el que la *NSA* recibió las copias de la mayoría de los telegramas internacionales que salieron del suelo norteamericano entre agosto de 1945 y mayo de 1975. En la expansión del programa fue esencial la cooperación de Agencias de comunicaciones transnacionales, como era el caso de *RCA Global*, *ITT World Communications* y *Western Union International*.[50]Aunque el número total de telegramas interceptados y leídos no es oficial, la *NSA* estima que en los últimos dos años de operatividad del programa fueron revisados un total de 150.660 telegramas. La obtención de los telegramas internacionales de ciudadanos estadounidenses implicó que durante treinta años se procediera sistemáticamente a la violación de la privacidad amparada en la Cuarta Enmienda,[51]que garantiza a los civiles el derecho a permanecer seguros frente a registros e incautaciones arbitrarios.

### 3.1.5. La Foreign Intelligence Surveillance Act (FISA). El mecanismo supervisor de inteligencia. [1978]

Durante sus intervenciones, el *Church Committee,* con el propósito de controlar las actividades de las principales Agencias de inteligencia del país lanzó una propuesta que adquirió forma durante el año 1978, ya en el contexto de la Administración Carter: la *Foreign Intelligence Surveillance Act* (*FISA)*. Una articulación jurídica que, en origen no se aplicaba fuera de territorio estadounidense y que regulaba los procesos para desarrollar una estrecha vigilancia tanto física como electrónica, y las funciones pertinentes de recopilación de información.

Todo ello orientado a lo que la propia Ley reconoce como los agentes que atentan contra la seguridad nacional (guiada por las perspectivas de la confrontación comunista durante la Guerra Fría): potencias extranjeras y agentes de tales potencias. No obstante, la Ley identifica también a personas civiles[52] estadounidenses y residentes en territorio

la *NSA*, especialmente en New York, donde más telegramas habían sido interceptados.

47 En respuesta a las presiones de la Casa Blanca, el *FBI* y la Fiscalía General, el Departamento del Ejército creó esta Unidad.
Committee Church: *National Security Agency Surveillance Affecting Americans*, Book III, 1976, pp: 745-746, en: http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_10_NSA.pdf

48 Ibíd., p. 739.

49 Ibíd.

50 Dos compañías internacionales de telegrafía: *RCA Global* e *ITT World Communications*. La tercera, *Western Unión International*, sólo proporcionó copias de cierto tráfico exterior a partir de 1945 hasta 1972.
Ibíd., p. 765.

51 *El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas*.
The Constitution of United States, *Amendment IV*, p. 5, en: https://www.uscg.mil/legal/mj/MJ_Doc/USConstitution.pdf

52 *Civiles estadounidenses significa: ciudadano de los Estados Unidos, extranjero admitido legalmente con residencia perma-*

americano como posibles amenazas- objetivo en caso de ser considerados como sospechosos de cualquier tipo de actividad relacionada con el espionaje o el terrorismo.[53]

Para poder imponer o acatar los preceptos de la Ley, el Comité decidió dotarle de su brazo ejecutor, el *Foreign Intelligence Surveillance Court (FISC)*,[54] como organismo concebido para la interpretación de la Ley y su cumplimiento así como elemento de concesión fundamental para las Agencias a la hora de obtener permisos de vigilancia, incluso cuando el objetivo solicitado en cuestión se encontrase fuera de Estados Unidos,[55]pero siempre que la adquisición de la información se llevara a cabo dentro de las fronteras norteamericanas.

Por último, el control y seguimiento de las funciones abarcarían todos los ámbitos dado que el Director de la Oficina Administrativa de los Tribunales de Estados Unidos estaba obligado por Ley a presentar anualmente a Comisiones y Comités específicos, el informe con detalle de las operaciones de inteligencia y espionaje, con el trabajo previo e involucrado del Director Nacional de Inteligencia en materia de desclasificación para evitar errores en el filtrado de informaciones.

### 3.1.6. La era del criptosecretismo: La NSA e IBM. El algoritmo Data Encryption Standard. [1970-1979]

Tal como indica Thomas R. Johnson, las tareas en materia de trabajo criptográfico de la *NSA* comenzaron de forma temprana, concretamente en la década de los 30.[56] Tras la Segunda Guerra Mundial y el reconocimiento de la criptografía como una herramienta esencial en el descifrado eficaz de Agencias extranjeras, la *NSA* comienza a potenciar el trabajo criptográfico aunque será especialmente a partir de la ubicación de los misiles en Bahía de Cochinos en 1962 cuando se potencien sus prestaciones.

Al mismo tiempo, continuaban avanzando los programas criptográficos en un intento de adaptar la Agencia al contexto bipolar de vigilancia. Resultado del progreso comenzaron los acuerdos con la compañía *International Business Machines Corp.* (*IBM*). A finales de los 60, el investigador Horst Feistel había conseguido desarrollar una línea de generadores que constituían un elemento clave en los ordenadores de *IBM* de cara al procesamiento de la información almacenada. El programa, llamado *Lu-*

*nente, una asociación o agrupación que incorpore un número considerable de miembros de los cuales parte sean ciudadanos de los Estados Unidos o extranjeros admitidos legalmente con residencia permanente; y empresas que operan desde territorio norteamericano.*
Public Law 511-95th Congress: *Foreign Intelligence Surveillance Act of 1978*, Title I: Electronic Surveillance within the United States for Foreign Intelligence Purposes, Sec. 101: "Definitions", October 25, 1978, p. 6, en: http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf

53 *Como salvaguarda, la Ley proporciona en caso de agravio a cualquier civil unos parámetros de compensación para cubrir el daño causado y que oscilan entre los 100 y los 1000 dólares por día de violación de los derechos del civil al ser sometido a los mecanismos de vigilancia de las Agencias.*
Ibíd., Sec. 110: "Civil liability".

54 *Cuyo Presidente designará públicamente 11 jueces de distrito, de los cuales no menos de 3 habrán de residir en 20 millas a la redonda del distrito de Columbia. Constituirán un tribunal que tendrá competencia para escuchar las solicitudes de vigilancia electrónica en cualquier lugar dentro de los Estados Unidos de conformidad con los procedimientos establecidos en la presente Ley.*
Ibíd., Sec. 103: "Designation of judges".

55 *El Foreign Intelligence Surveillance Court será competente para examinar una solicitud de vigilancia respecto a una persona de Estados Unidos que se crea razonablemente que se encuentra fuera de los Estados Unidos, para adquirir información de inteligencia extranjera.*
Ibíd., Title VII: Additional Procedures Regarding Certain Persons Outside the United Satates, Sec. 703: "Certain acquisitions inside the United States targeting United States persons outside the United States".

56 Y continuó a través de los años de la guerra y en los 50. En 1962, a raíz de la crisis de los misiles de Cuba, la Casa Blanca quería saber qué mercancías estaban viajando a Cuba. Esto implicó la transmisión de nombres e información vinculante a americanos y violó las reglas habituales de obtención de *SIGINT*. La idea resultó ser irresistible. En 1965, como resultado de las conclusiones de la Comisión Warren, el Servicio Secreto pidió a la *NSA* estar atenta en relación a ciertas personas que podrían ser una amenaza para el Presidente y que engrosaban sus *Watch Lists*.
Véase JOHNSON, R. Thomas: *American Cryptology during the Cold War; 1945-1989*, Book III, Series VI, Volume V, National Security Agency & Central Security Service, 2007, p. 84.

*cifer*, encontró su mejor aliado para expandirse en la encriptación bancaria del Banco Lloyd de Londres.[57]

Con el éxito de *Lucifer*, comenzó a surgir la idea en el seno del Gobierno estadounidense de que se requería de un sistema de encriptación estándar indescifrable poniéndose para ello en manos de la industria privada. Como recoge Johnson, las primeras ofertas resultaron del todo decepcionantes y por esta razón, la *NSA* comenzó a trabajar en su propio algoritmo de cifrado, aunque la colaboración entre Howard Rosenblum, subdirector de investigación e ingeniería, y Walter Tuchman, de *IBM*, fue clave para alcanzar el éxito.[58]En julio de 1977, el algoritmo *Data Encryption Standard* era ya una realidad.

A principios de la década de los 90 ya se había convertido en el algoritmo de cifrado más utilizado del mundo y aunque su exportación estaba completamente restringida, como indica Johnson, "*era ampliamente utilizado fuera de los Estados Unidos. Según un estudio de marzo de 1994, había 1.952 productos desarrollados y distribuidos en treinta y tres países*".[59]

Más allá de un sistema de intercambio de información en línea conocido como *Community On- line Information System* (*COINS*) creado en los 60 por la Agencia y la excesiva confianza en el programa *Autosevocom*,[60]un sistema engorroso y costoso muy limitado en acceso sólo para usuarios de alto nivel; no existen antecedentes tan importantes en el desarrollo de la criptografía que los de los setenta. Se trata de un período de desarrollo acelerado de los sistemas de software y en las bases de datos.

57 En el año 1971, el Banco Lloyd de Londres decidió ponerse en contacto con *IBM* para garantizar la seguridad de las transacciones. Ahí es donde entró en juego *Lucifer*, con objeto de encriptar las transacciones bancarias.
Ibíd., p. 232.

58 Howard Rosenblum descubrió que Walter Tuchman estaba trabajando en una modificación de *Lucifer* para uso más generalizado. La *NSA* dio a Tuchman financiación y lo llevó a trabajar de manera conjunta con la Agencia para que desarrollara su modificación del programa.
Ibíd.

59 Ibíd., p. 239.

60 Se trata del primer programa de la *NSA* orientado a la protección del teléfono del Departamento de Defensa. Debido a sus deficiencias, que afectaban a la calidad de escucha y voz de los terminales, ya a finales de la década de 1960, el departamento tuvo la esperanza de que la Agencia desarrollara algo mejor y decidió no continuar con la expansión de *Autosevocom*.

Ibíd., p. 142.

### 3.1.7. La Orden Ejecutiva 12333. Las 16 Agencias Ejecutivas de inteligencia. [1981]

Tras casi dos décadas velando por la construcción de una comunidad de inteligencia estructurada, después de sortear en el pasado los escándalos de vigilancia e instrumentación de las Agencias, y que amenazaron con derrumbar los principios de seguridad y de anticipación internacional construidos sobre la *National Security Act* de 1947; el 4 de diciembre de 1981, el Presidente Ronald Reagan firmaba la Orden Ejecutiva *12333*, por la que se actualizaba la estructura de la comunidad de inteligencia norteamericana en su conjunto.

La Orden sentó las bases sobre las que actuar en plena espiral de confrontación y la orientación de los esfuerzos de inteligencia,[61]además de reconocer las amenazas principales y distinguir en el espionaje, el terrorismo y las armas de destrucción masiva los núcleos de acción fundamentales.[62]

Como indica Pilar Pozo Serrano, la Orden Ejecutiva *12333* autorizó a las Agencias de inteligencia a realizar contratos y acuerdos para obtener servicios de compañías e instituciones privadas y a no revelarlos por razón de seguridad. Acuerdos que "*se extienden a los mandos militares gracias al Título 10 del Código Federal de Estados Unidos, que regula las fuerzas armadas, y que confiere al Secretario de Defensa la autoridad para establecer actividades comerciales necesarias para proporcionar seguridad a las acciones de obtención de inteligencia en el exterior*".[63]

Según lo compilado en esta Ley, la comunidad de inteligencia estará autorizada tanto a recopilar la información para el Presidente como a analizarla, producirla y difundirla teniendo siempre en cuenta en todas estas funciones el papel activo que ejerce el Secretario de Defensa,[64] quien retoma así el protagonismo otorgado en la estructura por medio de la enmienda a la *NSA* de 1949.

De este modo, la Ejecutiva *12333* conforma un brazo de inteligencia articulado por 16 Agencias de-

61 La Inteligencia de Estados Unidos proporcionará al Presidente, el *National Security Council* y el *Homeland Security Council* toda la información relativa a actuación exterior, defensa, y las políticas económicas, así como sobre la protección de los Estados Unidos y sus intereses frente a las amenazas de seguridad extranjeras. Todos los departamentos y Agencias cooperarán plenamente para cumplir con este objetivo.
Véase United States Government: *Executive Order 12333*, as Amended by Executive Orders *13284* (2003), *13355* (2004) and *13470* (2008), Preamble, Part I: Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts, 1.1 Goals, December 4, 1981, p. 1, en: https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf

62 La presente Orden tiene por objeto mejorar las técnicas de recolección humanas y técnicas, especialmente las llevadas a cabo en el extranjero, y la adquisición de la inteligencia extranjera significativa.
Ibíd., Preamble: Part 2: "Conduct of Intelligence Activities".

63 POZO SERRANO, Pilar: "Externalización de funciones de inteligencia: oportunidades y riesgos a la luz de la experiencia estadounidense", *Inteligencia y seguridad,* nº 6, 2009, pp: 197-222.

64 *El Departamento de Defensa. El Secretario de Defensa deberá:*
*a) (Incluso a través de medios clandestinos), analizar, producir y difundir información e inteligencia y ser sensible a tareas de recogida y de asesoramiento por el Director;*
*b) (Incluso por medios clandestinos), analizar, producir y difundir defensa e inteligencia relacionada con la defensa y contrainteligencia, según sea necesario para la ejecución de las funciones del Secretario.*
Véase United States Government: *Executive Order 12333*, op. cit., Preamble, 1.10 *The Department of Defense*, p. 11.

partamentales[65] dirigidas por el *NSC*,[66] destinado a apoyar en la toma de decisiones al Presidente, quien a su vez queda reconocido como la máxima autoridad en materia de inteligencia relacionada con la política interior y exterior norteamericana.

### 3.1.8. La Goldwater-Nichols Act. La reorganización del Department of Defense. [1986]

Entre 1958 y 1983 no hubo grandes cambios en la organización interna de la defensa norteamericana, a pesar de que hubo varios intentos[67] por conseguir, sobre todo, una mayor difuminación en la alianza entre el Congreso y los diferentes departamentos.[68]No obstante, en los años 80, tras el impulso de la Ejecutiva *12333*, Reagan emprenderá una reforma del *DoD* que sin duda será la más importante desde la aparición del mismo. El escenario del contexto previo al año 1986, en el que se promulgará la *Goldwater-Nichols Act*, arranca en 1972, con el convencimiento de muchos de los legisladores más influyentes acerca de la inoperancia y la ineficacia del *DoD* viendo el desarrollo traumático de la guerra de Vietnam, iniciada hacía ya diecisiete años.

Los estamentos más criticados por la traumática derrota que se venía produciendo en el frente fueron los líderes militares y el Gobierno, especialmente a la hora de contrarrestar la insurgencia norvietnamita. Este descontento generalizado implicó finalizar la presencia de líderes en la cadena de mando militar, en la campaña de Vietnam. En mayo de 1975,[69]dos meses después de la caída de Saigón, tuvo lugar el conflicto de Mayagüez, un carguero estadounidense reclamado como suyo por el Gobierno de los Jémeres rojos de Camboya, que trajo consigo el cautiverio de la tripulación. Estados Unidos organizó un rescate en el que involucró a todos los estamentos junto con las Agencias de inteligencia, en una operación que consistía en un asalto frente a la costa de Camboya, donde se creía que podían estar los cautivos. Sin embargo, la oportunidad se volvió a tornar en ineficacia. En el momento del ataque la tripulación había sido puesta en libertad, lo que provocó una confusión generalizada y un saldo de 20 muertos y 40 heridos entre el personal estadounidense. Como

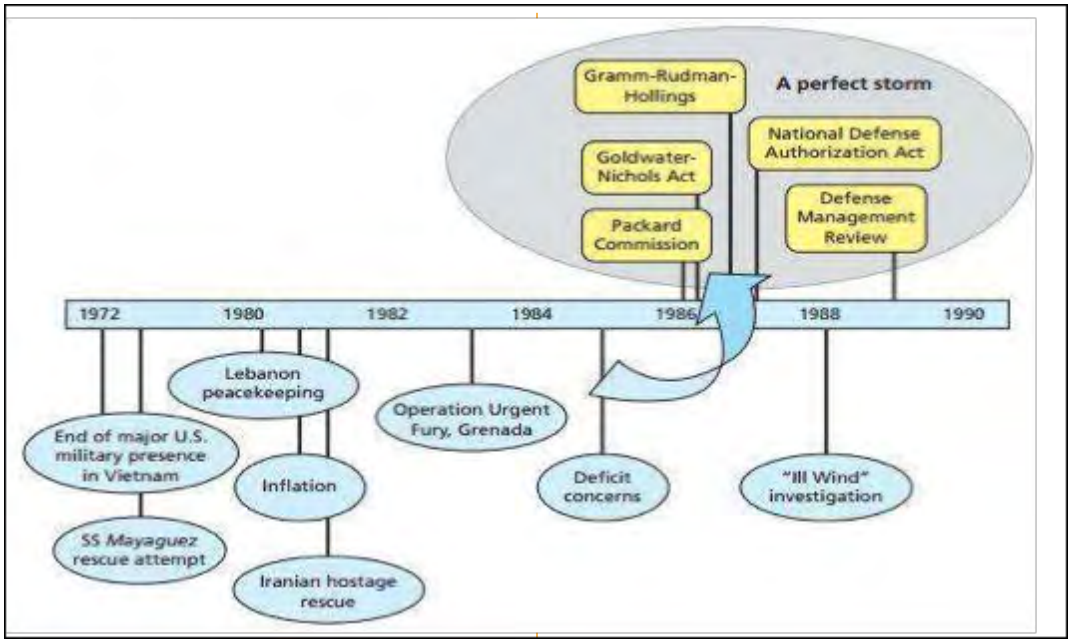
65 *Comunidad de inteligencia se refiere a:*
*(1) La Oficina del Director de Inteligencia Nacional;*
*(2) La CIA;*
*(3) La NSA;*
*(4) La DIA;*
*(5) La Agencia Geoespacial de Inteligencia Nacional ;*
*(6) La NRO;*
*(7) Las otras oficinas dentro del Departamento de Defensa dedicadas a la recolección de inteligencia extranjera a través de los programas de reconocimiento;*
*(8) Los elementos de inteligencia y contrainteligencia del Ejército, la Armada, la Fuerza Aérea y la Infantería de Marina;*
*(9) Los elementos de Inteligencia del FBI;*
*(10) La Oficina de Inteligencia de Seguridad Nacional de la DEA;*
*(11) La Oficina de Inteligencia y Contrainteligencia del Departamento de Energía;*
*(12) La Oficina de Inteligencia e Investigación del Departamento de Estado;*
*(13) La Oficina de Inteligencia y Análisis del Departamento de Hacienda;*
*(14) La Oficina de Inteligencia y Análisis del Departamento de Seguridad Nacional;*
*(15) Los elementos de inteligencia y contrainteligencia de la Guardia Costera; y*
*(16) Las demás elementos de cualquier Departamento o Agencia que puedan ser designados por el Presidente, o designado conjuntamente por el Director y el Jefe del Departamento u organismo interesado, como un elemento de la comunidad de inteligencia*.
Ibíd., Part III: General Provisions, 3.5 "Definitions", pp: 15-16.

66 *El National Security Council actuará como la más alta entidad directiva que proporciona apoyo al Presidente para la revisión de las pautas y la dirección de la conducta de toda la inteligencia extranjera, contrainteligencia y acción encubierta, y las políticas y programas concomitantes*.
Ibíd., Preamble, 1.2 "The National Security Council", pp: 1-2.

67 Hubo llamadas continuas hacia la reforma: el *Symington report* por John F. Kennedy, el *Blue Ribbon Defense Panel* de Richard Nixon, y los *Defense Organization Studies* de Jimmy Carter a finales de los años 1970, son muestra de ello.
Véase LOCHER III, R. James: "Has it worked? The Goldwater-Nichols Reorganization Act", *Naval War College Review*, Vol. LIV, nº 4, Autumn 2001, p. 99.

68 Según Locher, incluso Eisenhower, un héroe de guerra, fue incapaz de superar esta alianza, y acabó por convertirse en una lección importante para los Presidentes y Secretarios de Defensa posteriores.

69 1975 fue un año de importantes acontecimientos internacionales para Estados Unidos: además de la caída de Saigón y la crisis del Mayagüez, en ese mismo año tienen lugar la caída de Camboya a manos de los jémeres rojos, el inicio del programa de acción encubierta en Angola, el suministro de armas a los kurdos de Iraq como medida de apoyo al Sha de Persia, o las sanciones contra Turquía como consecuencia de su ocupación del norte de Chipre el año anterior.




Fuente: National Defense Research Institute.

resultado, el ejército de Estados Unidos fue criticado de nuevo, por su defectuoso servicio de inteligencia y los continuos problemas de comunicación.

La misma falta de comunicación[70] destacó igualmente a la hora de velar por la paz en el Líbano en el primer lustro de la década de los 80, en un momento en que se llevó a cabo en la nación insular de Granada, la operación *Urgent Fury*, y por medio de la cual se buscaba responder al golpe de Estado de Hudson Austin, favorecido por una alianza cubano-soviética. No obstante, aunque se acabó consiguiendo el propósito de la invasión volvieron a aparecer las mismas ineficacias operativas.[71]En definitiva, en 1986, Reagan cree necesario un nuevo balance del *DoD*, mediante la *Packard Commission*,[72]para evaluar las brechas en la organización y emprender las reformas necesarias.

A partir de la *Goldwater-Nichols Act*[73] de 1986, de reorganización del *DoD*, el establecimiento militar sufrió el conjunto más radical de reformas en materia de defensa en casi 40 años de existencia. Reformas que se reafirmarían posteriormente con la *National Defense Authorization Act* de 1987. La *Goldwater-Nichols Act* en su preámbulo, ya dejaba claro su propósito de reorganización del *DoD* para el fortalecimiento de la autoridad civil en detrimento de la propiamente militar y la mejora en

70 Una investigación determinó que seis cadenas de mando controlaban las acciones de la unidad anfibia de la Marina desplegada en el Líbano y que esto dio lugar a interrupciones en la comunicación y la autoridad no quedaba del todo clara. Los líderes políticos y militares también cambiaron con frecuencia las reglas de combate durante los dos años en los que estuvieron involucradas las fuerzas militares, lo que ayudó a crear una atmósfera de dudas entre los infantes de la Marina y que contribuyó a la muerte de 275 de ellos en un ataque terrorista.

Véase NEMFAKOS, Charles & BLICKSTEIN, Irv & MCCARTHY, Aine Seitz & SOLINGER, M. Jerry: *The Perfect Storm. The Goldwater-Nichols Act and its effect on Navy acquisition*, National Defense Research Institute, Occasional paper, RAND corporation, 2010, p. 7.

71 Las malas comunicaciones, el mando y el control, y la planificación, a pesar de los esfuerzos de las tropas sobre el terreno, disminuyeron la eficiencia operativa. Ibíd., pp: 7-8.

72 Creada por la Orden Ejecutiva *12526*, buscaba estudiar desde diferentes perspectivas la gestión del Departamento de Defensa. La Comisión concluyó entre sus recomendaciones en la necesidad de fortalecer la figura del Jefe de Estado mayor o que el presupuesto de defensa fuera aprobado por el Congreso de los Estados Unidos, cada dos años, en lugar de adjudicar una contabilidad anual a defensa.

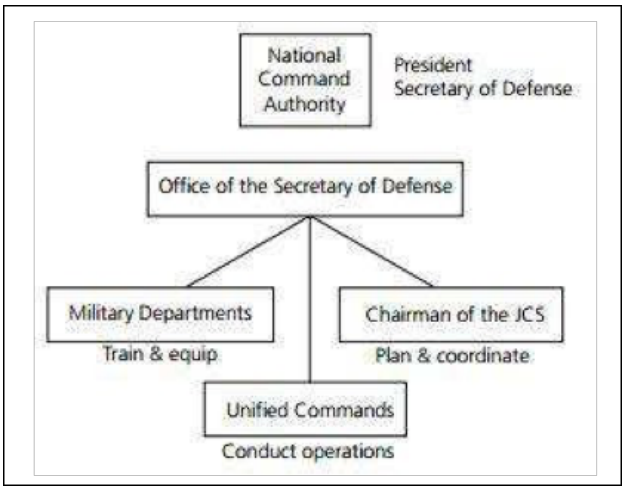
73 Recibe este nombre por los dos senadores: Barry Goldwater y William Flynt Nichols, encargados de redactar el Proyecto de Ley, firmado por Reagan el 1 de octubre de 1986.

el asesoramiento militar al Presidente y al *NSC*, así como al Secretario de Defensa. De este modo, la Ley lo que conseguirá es, por un lado, que el Jefe de la *Joint Chiefs of Staff (JCS)* sea el encargado de planificar y coordinar las acciones concernientes al *DoD* eliminando de la ecuación al establecimiento militar en cada uno de sus servicios (Fuerzas terrestres, aéreas y marítimas), quienes jugarán a partir de ahora el único protagonismo de recurso en manos del aparato de decisiones. Así, los líderes en la cadena de mando del *establishment* militar, pasarán a ser ahora, meros asesores del Presidente y del Secretario de Defensa, incluso, el Jefe de la *JCS* adquiere la responsabilidad de supervisar las actividades de los comandos de combate unificados, tarea antes exclusiva de los líderes militares de más elevado rango. En último lugar, el Secretario de Defensa deberá ser informado por el Jefe de la *JCS*,[74]y seguirá siendo así, el enlace directo con el Presidente.

## 3.2. La NSA en la post-Guerra Fría. [1991-2001]

### 3.2.1. El dividendo de la paz en la etapa Clinton y la puesta en marcha de la Revolution in Military Affairs. El impacto en la vigilancia del siglo XXI. [1993-2001]

Si bien la *Goldwater-Nichols Act* consiguió introducir las reformas más importantes en el seno del *DoD*, su eficacia no habría sido posible sin las relaciones internacionales norteamericanas del momento. Éstas se beneficiaron de la inserción de mayor autoridad civil en el departamento, así como del desplazamiento a un lado de los líderes militares, gracias sobre todo al deshielo de las relaciones soviético-estadounidenses tras la cumbre de Ginebra, celebrada en noviembre de 1985 entre Mijaíl Gorbachov y Ronald Reagan. Aunque en el comienzo de las conversaciones, el Presidente norteamericano se negara a dar marcha atrás en sus ambiciosos planes militarizadores, bautizados como "*la guerra de las galaxias*",[75]el camino no conduciría sino al deshielo definitivo de las tensiones, con el acuerdo *START I* en la cumbre de Moscú de 1989.[76]Un paso previo necesario para la declaración conjunta entre el sucesor de Reagan, George H. W. Bush, y el propio Gorbachov, el 3 de diciembre de 1989, en la cumbre de Malta, en la que se daba por zanjada la Guerra Fría.




Fuente: U.S. Naval War College.

Una de las primeras medidas en materia de defensa que llevó a cabo el sucesor de Reagan, fue la *Defense Management Review*, apenas un mes des-

74 *El Jefe de la Joint Chiefs of Staff de Estados Unidos es el principal asesor militar del National Security Council y del Secretario de Defensa.*
Public Law 433-99th Congress: *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, Chapter V: Joints Chiefs of Staff, Sec. 151: "Joint Chiefs of Staff: composition; functions", October 1, 1986, p. 15, en: http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf

75 La iniciativa de defensa estratégica de Reagan fundamentada en la expansión militar de las capacidades norteamericanas, para disuadir al oponente soviético, por medio de la fortaleza nuclear, empleando armas balísticas estratégicas.

76 El *Strategic Arms Reduction Treaty* estableció limitaciones en el número de misiles nucleares de cada superpotencia. El éxito de este acuerdo ha de entenderse como respuesta al repliegue que la URSS comenzó a dar desde 1988. A partir de esa fecha, gradualmente, la URSS fue notificando a sus aliados el final de su apoyo militar y económico. Así, Fidel Castro en Cuba, los sandinistas nicaragüenses en América Latina; los regímenes de Angola, Mozambique y el general Mengistu en Etiopía; Vietnam en Asia, etcétera; todos fueron informados del fin de la cooperación soviética. Este paso estratégico hacia atrás encuentra su reafirmación el 8 de febrero de 1988, cuando la URSS se comprometió a retirar sus tropas de Afganistán, haciendo efectiva su retirada el 15 de febrero de 1989.

pués de tomar el cargo de Presidente. En su informe de recomendación se perseguía conformar un aparato de defensa e inteligencia nacional, capaz de plasmar los criterios de la *Packard Commission* y redoblar los esfuerzos para la mejora en la gestión interna del departamento.[77]

Cuando Bill Clinton llegó a la presidencia norteamericana en 1993, lo primero que se encontró fue la gran factura de la política liberal de Reagan y el continuismo conservador de Bush. Los Presidentes republicanos habían disfrutado de una Administración con fuerte crecimiento económico, gracias a la bajada de impuestos y el aumento del gasto público para sufragar la Guerra Fría, especialmente en la Administración del primero. En el otro extremo, se encontraba una deuda pública desbordante, que había sido desatendida. A pesar de que Clinton ha pasado a la historia como uno de los Presidentes que más logró reducir la deuda y equilibrar las cuentas, es importante entender que entre 1987 y 1994,[78]la reducción de los gastos militares comenzó a erigirse como responsable del crecimiento económico de los Estados Unidos. Así pues, Clinton se benefició claramente del conocido como *Dividendo de la paz*, el resultado económico de la desmilitarización entre las dos potencias tras el fin de la Guerra Fría y especialmente tras la caída del bloque comunista. De hecho, la estabilidad del crédito en el país hizo posible una fuerte entrada de flujos internacionales a partir de 1995, hecho que inició el segundo gran ciclo al alza del dólar en el mundo.[79]

Desde el enfoque puramente militar, la victoria norteamericana en la guerra del golfo pérsico,[80]iniciada en agosto de 1991 y finalizada en febrero de 1992, puso de manifiesto el prototipo de guerra para el futuro.[81]De este modo, la rápida victoria en el conflicto de la coalición liderada por Estados Unidos sugiere la puesta en marcha de una *Revolution in Military Affairs* (*RMA*),[82]resultado de la expansión del sector en la etapa Reagan. El incremento de las inversiones en el aparato militar junto con la época de crecimiento económico en la etapa anterior al deshielo de las relaciones URSS-EEUU, se tradujeron en la Administración Clinton, tras la desmilitarización por la paz, en una reasignación de fondos y recursos que consiguió aumentar las prestaciones y la tecnología disponibles en manos de los diferentes servicios militares.

77 *El esfuerzo de defensa de EEUU se va a gestionar de tal manera que: asegure la continua fortaleza y la disposición de las Fuerzas Armadas de la nación; nos ayude a adquirir nuevos sistemas de armas a un menor coste, en menos tiempo y con mayores garantías de rendimiento; anime a la industria y el Gobierno por igual para satisfacer los más altos estándares de integridad; y promueva una mayor credibilidad del público hacia nuestra gestión de los recursos de defensa*.
CHENEY, Dick: *Defense Management. Report to the President*, Secretary of Defense, Washington, July 1989, p. 1, en: http://www.ndia.org/Advocacy/AcquisitionReformInitiative/Documents/1989_Defense_Management_Review.pdf

78 Los gastos militares del mundo disminuyeron a razón del 3,6% anual, lo que representó un ahorro acumulado de
935.000 millones de dólares, de los cuales, 810.000 millones correspondieron a los países industrializados y 125.000 millones a los del mundo subdesarrollado.

79 Coincidiendo además con una serie de crisis financieras internacionales que allanaron el terreno para la economía norteamericana. Primero en Japón, en 1990, y después en México en 1994 y Rusia en 1998. De este modo, Clinton

80 Conocida comúnmente como "*Operación Tormenta del Desierto*", que fue el nombre en clave de la respuesta militar norteamericana a la invasión iraquí del Estado de Kuwait.

81 *Tormenta del Desierto"* demostró que una ventaja importante de las fuerzas de Estados Unidos era su capacidad de ejecutar operaciones complejas en muy poco tiempo, que impidieron al enemigo responder. Esta ventaja se produjo no sólo gracias a sensores avanzados y municiones convencionales avanzadas, sino tal vez a una organización moderna, un mejor control y unas comunicaciones e inteligencia de sistemas y tecnologías que permitieron que la coalición liderada por Estados Unidos pudiera llevar a cabo esas operaciones de forma simultánea.
Véase DAVIS, C. Norman: "An Information-Based Revolution in Military Affairs", *Strategic Review*, U.S. Strategic Institute, Vol. 24, nº 1, Winter 1996, p. 85.

82 Los primeros estudios hablaron de una "revolución técnica militar" (*MTR*), aunque la mayoría de los analistas definen un *RMA*, es decir, en "asuntos militares" como un "aumento discontinuo en la capacidad militar y la eficiencia" que surge del cambio en la tecnología, los sistemas, los métodos operativos y las organizaciones militares.
Véase METZ, Steven & KIEVIT, James: *Strategy and the Revolution in Military Affairs: from theory to policy*, Strategic Studies Institute, US Army War College, June 27, 1995, p. 5.

Los analistas consideran que la corriente *RMA* tiene dos etapas: una que otorga el protagonismo al dominio de la información, la mejora de las comunicaciones o el uso de coaliciones; y otra basada en la robótica, la ciberdefensa o la nanotecnología,[83]sin duda un camino que comenzaba a introducir a Estados Unidos en la vigilancia global en pleno siglo XXI.

## 3.3. La NSA en el siglo XXI. Del 11-S a las revelaciones de Edward Snowden. [2001-2013]

### 3.3.1. Administración George W. Bush. [2001-2009]

#### 3.3.1.1. Global War on Terror. Las estructuras de seguridad e inteligencia de Estados Unidos al servicio de la GWT.

Tal vez por la cadena de fallos interna en un sistema creado para ser capaz de minimizarlos al máximo (a pesar de la inexistencia del Estado absoluto de seguridad), el Presidente Bush, a comienzos de 2002 y todavía bajo el shock de los ataques, autorizaba bajo iniciativa personal de su Vicepresidente primero Dick Cheney y Michael Hayden al frente de la *NSA*, a monitorizar,almacenar y analizar sin orden judicial previa, las llamadas telefónicas y los correos electrónicos de aquellos ciudadanos, estadounidenses o no, sospechosos de tener algún nexo con Al-Qaeda. Como señala Adolfo Hernández Lorente, un año después, amparándose en esta orden presidencial, conocida como la *Homeland Security Act,*[84]los servicios de inteligencia espiaron el flujo comunicativo de los países miembros del Consejo de Seguridad de Naciones Unidas, "*durante los días previos a la votación de la Resolución 1441 (2002) que supuestamente debía autorizar la guerra de Irak*".[85]Esto implicó espiar a países en principio aliados, como Francia o Brasil.

La vigilancia masiva comenzaba sin conocer aliados ni miramientos de confianza, una práctica que en realidad tiene su punto de partida en los momentos inmediatamente posteriores al 11-S cuando Bush procede el 26 de octubre de 2001 a la firma de la *USA PATRIOT ACT*.[86]

**Ley Patriótica. USA PATRIOT ACT.** [2001]

Desde su promulgación, la *USA PATRIOT ACT* se erigió como la más polémica de la Administración Bush. La Ley perseguía dotar al aparato de Estado, pero sobre todo, a la inteligencia, de la eficiencia que había demostrado no tener en los ataques del 11-S. Todavía con el trauma de los devastadores acontecimientos, el espíritu de la Ley no es otro que subordinar los derechos ciudadanos a la vigilancia con objeto de incrementar la seguridad del Estado. Como señala Gustavo Díaz Matey, la *USA PATRIOT ACT* consistió en una "*disminución de la capacidad de los ciudadanos estadounidenses para obtener información sobre su Gobierno y, al mismo tiempo, le dio al Gobierno los medios para husmear en la vida personal de los mismos ciudadanos*".[87]Al comienzo de la propia Ley, se reconoce la necesidad de poner freno a la oleada de terror y violencia desatada tras el ataque de norteamericanos con relación

83 bíd., p. 6.

84 La *Homeland Security Act*, aprobada en noviembre de 2002, creó el *Department of Homeland Security* y la nueva posición a nivel de gabinete del *Secretary of Homeland Security*. Es importante entender esta reorganización del Gobierno federal como la mayor desde la creación del *Department of Defense*, a su vez por la enmienda de 1949 implementada en la *National Security Act* de 1947.

85 Lorente Hernández, Adolfo & Chamorro Fojón, Enrique & Piella Colom, Guillem: "Vigilados por defecto", *Instituto Español de Estudios Estratégicos* (*IEEEs*), nº 34, 4 Abril, 2014.

86 También conocida como *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.*

87 Por ejemplo, la Ley incluye cambios en las Leyes que regulan la vigilancia, por lo que es fácil para el Gobierno reunir subrepticiamente información sobre los individuos. Esta Ley desmantela el servidor de seguridad reglamentaria que separaba la inteligencia interna y externa, que se erigió a raíz de las investigaciones sobre los abusos de inteligencia en el caso Watergate. De hecho, la *CIA* y el *FBI* se encuentran ahora mucho más libres a la hora de compartir información.
Véase DÍAZ MATEY, Gustavo: "The U.S. Intelligence Reform and the National Intelligence Strategy of October 2005", *Revista UNISCI*, nº 10, Enero 2006, p. 361.

a los ciudadanos de origen o apariencia musulmana o directamente foránea.[88]

Por su parte, uno de los aspectos más importantes de la Ley es el reconocimiento de la actividad de información de inteligencia extranjera como una tarea que puede involucrar tanto a personas de Estados Unidos como de fuera del territorio norteamericano, relacionándose con organizaciones que persiguen el ejercicio de sabotajes, prácticas terroristas u otros actos hostiles contra la nación. De este extracto se extraen dos conclusiones fundamentales del acta. La primera es, que como se viene afirmando, los civiles estadounidenses podrán convertirse en objetivo de la comunidad de inteligencia y recibirán un trato similar al terrorista ubicado fuera de las propias fronteras, siempre que los indicios apunten a ello. Un hecho que dota de mayor maniobrabilidad y abandona de recelos de espionaje tanto a *CIA* como a *NSA*.

El segundo factor clave, es la asunción de que la Ley por más de tratarse de un instrumento legislativo nacional, tiene profunda implantación en las tareas internacionales de seguimiento terrorista de las Agencias de inteligencia. En otras palabras, una Ley nacional que posibilita la operatividad más allá del territorio nacional.[89]Pero donde finalmente se consagra la esencia de la *USA PATRIOT ACT*, es por medio de la Sección 215,[90]por medio de la cual se prohíbe tanto a particulares como a empresas que hayan recibido orden judicial de cooperación con las Agencias, la divulgación de la existencia de esa orden. Un panorama del que se aprovechará la *NSA* cuando construya sus programas de vigilancia y que le hará controlar de forma más influyente[91] a las corporaciones empresariales "*facilitadoras*" de información, como es el caso de *Microsoft*, entre otras.

para preservar su seguridad; (2) cualquier acto de violencia o discriminación contra cualquier estadounidense debe ser condenado; y (3) la nación está llamada a reconocer el patriotismo de los conciudadanos de todos los orígenes étnicos, raciales y religiosos.

Public Law 56-107th Congress of the United States of America: *USA PATRIOT ACT 2001*, October 26, 2001, Title I: Enhancing Domestic Security Against Terrorism, Sec. 102: "Sense of Congress condemning Discrimination Against Arab and Muslim Americans", en: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

**Los fallos en la inteligencia reconocidos en el 9/11 Commission Report.** [2004]

El 11 de septiembre de 2001 permanece en el imaginario colectivo como el acontecimiento más impactante y el acto de bienvenida más dramático del nuevo siglo. La configuración geoestratégica mundial, con el comienzo de la "*Global War on Terror*", (*GWOT*)[92]la reordenación de las amenazas

88 *(1) Los derechos civiles y las libertades civiles de todos los estadounidenses, incluidos los árabes americanos, los musulmanes, y los americanos del sur de Asia, deben ser protegidos, y deben tomarse todos los esfuerzos posibles*

89 *Para cualquier investigación con objeto de reunir información de inteligencia extranjera o información relativa al terrorismo internacional y para cualquier investigación con objeto de obtener información de inteligencia extranjera, no en relación con una persona de Estados Unidos o para proteger contra el terrorismo internacional o actividades clandestinas de inteligencia.*
Ibíd., Title II: Enhanced Surveillance Procedures, Sec. 214: "Pen Register And Trap And Trace Authority Under FISA".

90 Ibíd., Sec. 215: "Access To Records And Other Items Under The Foreign Intelligence Surveillance Act".

91 La *PATRIOT ACT* era tan polémica porque, cuando fue aprobada tras el atentado del 11 de septiembre, la sección 215 rebajó los estándares que debía cumplir el Gobierno para obtener "documentos comerciales/profesionales" desde "causa probable" a "pertinencia". Lo cual significaba que, para obtener documentos muy delicados o invasivos – como historiales médicos, transacciones bancarias o llamadas telefónicas-, el *FBI* solo tenía que demostrar que esos documentos eran "pertinentes" para una investigación en curso.
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 43.

92 A raíz del 11 de septiembre de 2001, después de los ataques terroristas de Al-Qaeda en los Estados Unidos, el Gobierno de EEUU declaró una guerra global contra el terrorismo. La naturaleza y los parámetros de esa guerra, sin embargo, siguen siendo poco claros y frustrantes. La Administración ha identificado una multiplicidad de

internacionales y lo más importante, la sensación global de que el estandarte más seguro del mundo se podía ver atacado, se constituyeron rápidamente en las creencias extendidas y en los pilares que cercaban la seguridad del siglo XXI.

No obstante, desde la perspectiva de la inteligencia norteamericana es relevante plantearse cuestiones acerca de su eficiencia, debido a que todo un amplio organismo, construido desde 1947 no hubiera servido para prever o anticipar el ataque terrorista múltiple. En otras palabras, el sistema falló, tal como se encargó de señalar el propio *9/11 Commission Report* de 2004.[93]Como indica Manuel Coma, el informe sacó a la superficie los fallos, deficiencias y errores en el trabajo "*de ese aparato de inteligencia que les cuesta a los contribuyentes americanos 40.000 millones de dólares al año, el 80% controlado, de forma más o menos indirecta, por el Departamento de Defensa*".[94]

Antes del 11-S, algunas Agencias como la *NSA* o la *NRO* veían limitados sus esfuerzos de vigilancia electrónica fundamentalmente por el retraso tecnológico de las organizaciones. Además, la falta de cooperación interdepartamental era la nota predominante en el día a día. Durante la década de los 90, las Agencias de inteligencia encargadas de velar por la evolución terrorista controlada eran la *CIA*, la *NSA* y el *FBI*. Las dos primeras adquirieron tempranamente, por su estructura, una naturaleza de enfoque de las amenazas a nivel internacional y a pesar de que había informes que avisaban de la posible amenaza terrorista en territorio norteamericano, siempre se creyó entre los propios departamentos, que al tratarse de amenazas en suelo nacional, las competencias recaían sobre el *FBI*. A pesar de las informaciones obtenidas[95] en las operaciones desarrolladas por la *NSA* acerca de la proximidad de ataque a Estados Unidos, la *NSA*, por iniciativa[96]de su Director, el propio Hayden, decidió mantener una línea fronteriza de actuación, todo ello a pesar de que con una simple orden del Tribunal *FISA* ya hubiera podido actuar.

Tanto la *CIA* como la *NSA* eran Agencias mucho más recelosas en relación al monitoreo de los ciudadanos estadounidenses, algo que resulta contraproducente dados los intentos de vigilancia en el pasado sobre suelo americano.[97]Se confería así la responsabilidad al *FBI*, quien no tenía la capacidad analítica para evaluar la vulnerabilidad del Estado si no era con los datos obtenidos de otras Agencias como la *CIA* o la *NRO*.

A ello hay que sumar que a pesar de que imperaba un espíritu de coordinación en las tareas gracias al acuerdo del 26 de agosto de 1977[98] con Inman

enemigos, incluyendo Estados delincuentes; proliferadores de armas de destrucción masiva; organizaciones terroristas de alcance mundial, regional y nacional; y el terrorismo en sí.
Véase RECORD, Jeffrey: *Bounding the Global War On Terrorism*, Strategic Studies Institute, Ed: Lulu, December 2003.

93 The National Commission on Terrorist Attacks Upon the United States: *The 9/11 Comission Report, 2004*, en: http://avalon.law.yale.edu/sept11/911Report.pdf

94 COMA, Manuel: "Fallos de inteligencia y responsabilidades gubernamentales", *Fundación para el Análisis y los Estudios Sociales (FAES)*, Cuadernos de pensamiento político nº 4, Octubre-Diciembre 2004, p. 118

95 La *NSA*, por ejemplo, informó de al menos 33 comunicaciones que indicaban un posible ataque terrorista inminente, ya en 2001. Altos funcionarios del Gobierno de Estados Unidos fueron aconsejados por la comunidad de inteligencia entre el 28 de junio y 10 de julio de 2001, acerca de la proximidad del ataque, alegando que podría "tener consecuencias dramáticas o causar un gran número de bajas".

Véase 107th Congress, 2d Session, The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence: *Report of the joint inquiry into the terrorist attacks of September 11, 2001*, December 2002, p. 7, en: https://fas.org/irp/congress/2002_rpt/911rept.pdf

96 Hayden testificó que era más apropiado para el *FBI* llevar a cabo dicha vigilancia porque la *NSA* no quería ser percibida como la Agencia encargada de la vigilancia doméstica y porque la inteligencia producida sobre comunicantes en los Estados Unidos es probable que involucre a actividades domésticas.
Ibíd., pp: 73-74

97Véase tanto en el desarrollo de programas como *SHAMROCK* o *MINARET* donde ambas Agencias (*CIA* y *NSA*) cooperaban, por ejemplo en la interceptación del flujo de telegramas internacionales; así como dentro del propio *FBI*, con el programa *COINTELPRO*, orientado a paliar la disidencia entre la población norteamericana.

98 El 26 de agosto de 1977 se lanza el "tratado de paz" entre las Agencias *NSA* y *CIA* con mediación del Director de

como mediador, entre la *CIA* y la *NSA* volvieron a aparecer antiguas fricciones[99]debido a la duplicidad de tareas, algo que incluso continuó después del ataque terrorista. Tal como incide Coma, uno de los temas más polémicos es si hubo descuido por parte del Gobierno en no prestar atención a las señales de alarma que la Inteligencia, a pesar de no haber sido capaz de conectar por su falta de coordinación, sí que estuvo enviando al Gobierno.[100]

Lo que parece claro es que junto con la confusión departamental y la falta de atención gubernamental, otra de las grandes limitaciones de la *NSA* en el lustro previo al 11-S continuaban siendo las fórmulas de trabajo de sus analistas. A pesar de la cantidad ingente de material recogido y compilado por la organización, las herramientas y las bases de datos disponibles no impedían que fueran los propios trabajadores[101] los que, empleando sus propios filtros de atención personal, acabaran seleccionando lo considerado como altamente peligroso o posible amenaza terrorista. La falta de asimilación tecnológica entre los analistas se erigió así en brecha determinante para el escape de información esencial sobre el ataque.

**El impacto de la Intelligence Reform and Terrorism Prevention Act.**

[2004]

El 17 de diciembre de 2004, la Administración Bush promulga, previo paso por el Congreso, la *Intelligence Reform and Terrorism Prevention Act*, un texto que persigue la reforma de la estructura de la comunidad de inteligencia bajo la nueva figura del *Director of National Intelligence*. Nombrado por el Presidente, con el consentimiento del Senado, el Director de Inteligencia Nacional, actuará como el principal asesor[102] del Presidente y del *NSC* en materia de seguridad nacional, al constituirse como Jefe de los servicios de inteligencia. Del mismo modo, en la Ley se especifica la prohibición de ejercer más funciones que las de su propio cargo, es decir, el Director de Inteligencia Nacional no podrá ser a la vez el Director de ninguna de las Agencias de inteligencia que queden bajo su responsabilidad.

De la misma manera, el texto diferencia bajo las competencias de su cargo, en un primer nivel, entre el *National Counterterrorism Center* (*NCTC*), la *Privacy and Civil Liberties Oversight Board* (*PCLOB*) y el *National Counterproliferation Center* (*NCPC*).

la *NSA* Bobby Inman, quien coincidiendo con la llegada a la presidencia de Jimmy Carter (1977-1981); releva al frente de la Agencia al General Lew Allen. El acuerdo confería, con objeto de evitar futuras colisiones, que el agente centralizador de las tareas de *SIGINT* será la *NSA*.

99 La *CIA* percibía de la *NSA* un intento de querer controlar la implementación y desarrollo de la tecnología, mientras que la *NSA* estaba preocupada acerca de que la *CIA* llevara a cabo operaciones de inteligencia *SIGINT*, conferidas a la *NSA*. Estas fricciones persistieron incluso después de los ataques del 11 de septiembre. En los primeros seis meses de 2002, por ejemplo, no menos de siete memorandos de nivel ejecutivo (uno de ellos del Presidente) se emitieron para delimitar las responsabilidades y autoridades tanto de la *CIA* como de la *NSA*.
Véase 107th Congress, 2d Session, The House Permanent Select Committee on Intelligence, op. cit., p. 75

100 Tal como señala Coma, sin entrar en una cuestión tan vidriosa, lo importante es señalar que la correspondiente Comisión concluye que aunque se le hubiera dado una atención preferente, de todas formas no hubiera bastado para prevenir los atentados.
Coma, "Fallos de inteligencia" op. cit., p. 123

101 En ausencia de herramientas más sofisticadas, los analistas de la *NSA* debían aún realizar la mayor parte de su trabajo con lápiz y papel. Muchos desarrollaban sus propias bases de datos. De hecho, el programa *TRAILBLAZER*, muy publicitado internamente en la *NSA*, fue citado a menudo por los funcionarios de la Agencia como la solución a muchos de estos problemas.
Véase 107th Congress, 2d Session, The House Permanent Select Committee on Intelligence, op. cit., p. 55.

102 *A menos que se indique lo contrario por el Presidente, el Director de Inteligencia Nacional tendrá acceso a toda la inteligencia nacional y la inteligencia relacionada con la seguridad nacional que se recoge por cualquier Departamento Federal, Agencia u otra entidad, salvo las excepciones establecidas por la Ley o, en su caso, bajo las directrices acordadas por el Fiscal General y el Director de Inteligencia Nacional.*
Véase Public Law 458-108th Congress: *Intelligence Reform and Terrorism Prevention Act of 2004*, Title I: Reform of the Intelligence Community, Sec. 102: "Responsabilities and authorities of the Director of National Intelligence", December 17, 2004, p. 8, en: http://www.nctc.gov/docs/irtpa.pdf

El *NCTC* se encarga de llevar a cabo la planificación operativa estratégica en materia antiterrorista, que incluye, la definición de misiones, objetivos, asignación de funciones al personal de las Agencias, así como la vigilancia en la adecuada coordinación interinstitucional.[103]Por su parte, la *PCLOB*, integrada por un Presidente y un Vicepresidente, desempeña tareas relacionadas con la garantía de que las libertades relacionadas con la privacidad y los derechos civiles sean considerados adecuadamente en la aplicación de Leyes, reglamentos y políticas, elaborados por el poder ejecutivo en relación con los esfuerzos para proteger a la nación contra el terrorismo.[104]Finalmente, el *NCPC*, orientado a la detención en la proliferación de armas de destrucción masiva, y de obligatoria conformación a más tardar 18 meses después de la fecha de entrada en vigor de la Ley.

**Revisión de la USA PATRIOT ACT.** [2005]

En un intento de reajustar, que no prohibir, una Ley como la *USA PATRIOT ACT*, profundamente marcada por el trauma reciente del 11-S, en julio de 2005, el Senado sometió a una serie de cambios al texto, aunque las esperanzas de los grupos en contra[105] de la Ley se desvanecieron de inmediato al ver que la esencia central de coacción del documento continuaría ejerciendo su influencia sobre la población.

Una de las modificaciones más importantes fue la relacionada sobre las secciones de registro empresarial del *FISC*, con objeto de autorizar al Director del *FBI* o a una persona designada por él, a solicitar al tribunal la emisión de órdenes[106] amparadas por la Sección 215 y que permite al Gobierno obtener información sobre todo tipo de materiales tangibles.[107]

Del mismo modo, en la revisión de 2005, se garantizó el endurecimiento de la Ley en materia de recopilación de metadatos en manos de los servicios de inteligencia. Después del 11-S, la *NSA* comenzó a implantar un programa de investigación electrónica en suelo norteamericano, amparado por la *USA PATRIOT ACT*, que posibilitaba la recopilación de los metadatos de múltiples llamadas telefónicas, esto es, sin acceso al contenido, pero detallando la información sobre el número marcado, la llamada desde el número de origen, la fecha, hora y duración. Mediante la renovación de 2005, a pesar de la prohibición marcada por la Cuarta Enmienda a la hora de ejercer registros e incautaciones de modo indiscriminado, el Senado garantizó una mayor protección a las prácticas de las Agencias. Cabe adelantar que las promesas conferidas por Obama cuando alcanzara la presidencia en 2009 sobre el reajuste de este programa, no afectaron en gran medida al trabajo de conservación y registro de metadatos de la *NSA* en comparación a la Administración Bush.

---

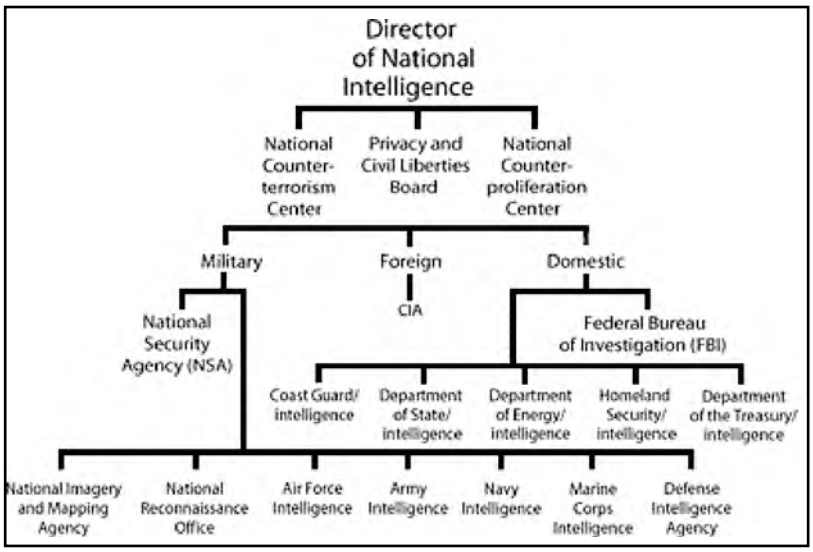
103 El Director del *NCTC* supervisará la ejecución de los planes operativos estratégicos y deberá obtener la información pertinente de los departamentos y organismos sobre el avance de dichas entidades en la ejecución de los planes.
Véase COLLINS. M. Susan: *Summary of Intelligence Reform and Terrorism Prevention Act of 2004*, United States Senate Committee on Governmental Affairs, December 2004, p. 8.

104 Las responsabilidades de la *PCLOB* abarcan tanto el consejo y la supervisión como la revisión de las regulaciones y políticas, incluidas las directrices de intercambio de información y la prestación de asesoramiento al Presidente y los departamentos y Agencias de la rama ejecutiva. Se pedirá a la Junta que informe al menos anualmente al Congreso de sus principales actividades. [...] Sólo si la información solicitada, para proteger los intereses de seguridad nacional, debe omitirse, según lo determinado por el Director de Inteligencia Nacional, en consulta con el Fiscal General, la información puede ser retenida.
Ibíd., pp: 6-7.

105 Una minoría de senadores del ala conservadora pero sobre todo senadores demócratas percibían el peligro y el abuso de poder de la Ley desde su aprobación en 2001.

106 Bajo la Sección 215, el *FBI* puede solicitar al *FISC* una orden que afecta a toda persona capaz de producir "cualquier cosa tangible" si existen motivos razonables para creer que las cosas buscadas son relevantes en relación a actividad de inteligencia extranjera, terrorismo internacional o espionaje.
Véase LIU, C. Edward, & NOLAN, Andrew, & THOMPSON, M. Richard: *Overview of Constitutional Challenges to NSA Collection Activities*, Congressional Research Service, CRS Report, May 21, 2015, p. 2, en: https://www.fas.org/sgp/crs/intel/R43459.pdf

107 La Ley incluso especifica lo que entiende por este tipo de material tangible: "libros, registros, papeles, documentos y otros artículos similares".




Fuente: u-s-history.com

**El camino a la Ley de enmiendas FISA.** Las reformas de 2006: *Terrorist Surveillance Act*, *Electronic Surveillance Modernization Act* y *Protect America Act*.

La Ley *FISA*, nacida como mecanismo de control de vigilancia de las Agencias de inteligencia como resultado del *Church Committee,* en 1978, con el tiempo, debido a la evolución de la amenaza terrorista, se ha erigido en factor posibilitador del Gobierno norteamericano desde el plano legal y en una perfecta armonía con la *USA PATRIOT ACT*. Todo ello, para poner en manos de sus servicios de inteligencia las herramientas de vigilancia y monitorización necesarias.

Ha sido modificada en varias ocasiones tras los atentados del 11-S. La primera de estas reformas tuvo lugar el 16 de marzo de 2006 cuando los senadores Mike DeWine, Lindsey Graham, Chuck Hagel y Olympia Snowe introdujeron en la propia Ley una categorización similar bajo el título: "*Terrorist Surveillance Act*". Con este primer reajuste, se dotaba al Presidente de una autoridad adicional[108] para llevar a cabo las actividades de vigilancia electrónica de presuntos terroristas sujetos a la supervisión del Estado e incluidos en las listas de vigilancia como potenciales amenazas.

El 18 de julio del mismo año, la senadora Heather Wilson, halló el perfecto complemento de esta primera enmienda en la Ley, con la inserción de la "*Electronic Surveillance Modernization Act*", un texto que aumentaba la autoridad presidencial hasta convertirle, por medio de la Fiscalía General en el centro[109] de la vigilancia electrónica sin necesidad de previa orden judicial, de toda la actividad derivada de las llamadas telefónicas internacionales y el correo

108 El Presidente determina que la vigilancia es necesaria para proteger a los Estados Unidos, sus ciudadanos, o sus intereses, ya sea dentro de los Estados Unidos o fuera de los Estados Unidos. [...] El Presidente deberá establecer y mantener a los efectos de esta Ley, una lista de grupos y organizaciones que están sujetas a la vigilancia electrónica autorizada bajo el *Terrorist Surveillance Program*. La lista se conoce como la *Terrorist Surveillance List*.
Véase 109th Congress-2d Session, DEWINE, Mark, & GRAHAM, Lindsey, & HAGEL, Chuck, & SNOWE, Olympia: *Terrorist Surveillance Act of 2006*, 2006, pp: 2-8.

109 Establece que el Presidente, a través del Fiscal General, podrá autorizar la vigilancia electrónica sin una orden judicial en el título I de la *FISA*, para adquirir información de inteligencia extranjera por períodos de hasta a un año, si el Fiscal General certifica por escrito bajo juramento que la vigilancia electrónica está dirigida a la adquisición de los contenidos de las comunicaciones de una "potencia extranjera", como se define en la sección 101 (a).
Véase BAZAN, B. Elizabeth: *Electronic Surveillance Modernization Act*, as Passed by the House of Representatives, CRS Report for Congress, Legislative Attorney American Law Division, January 2007, p.8.

electrónico de grupos armados terroristas identificados en previsión de posibles amenazas a la nación.

La siguiente reforma tuvo lugar el 28 de julio de 2007, bajo la denominación de *Protect America Act*. Con esta incorporación a la Ley *FISA*, se pretendía que la propia estructura legal amparase al Gobierno a intervenir las comunicaciones [110]extranjeras sin supervisión del Tribunal *FISA*.

Por último, el 20 de junio de 2008, tras dotar a la Ley *FISA* del aparato protector necesario con las sucesivas reformas previas, otorgando un papel decisivo para el Presidente y enmendando los conatos de las Agencias de inteligencia de intervenir e interceptar las comunicaciones foráneas, se aprobó en el Congreso por 293 votos a favor por 129 en contra, la *FISA Amendments Act*. Con esta última reforma, los tiempos asignados por defecto a la vigilancia electrónica se dispararon, llegando a alcanzar el año de duración, a pesar de que en las propias actividades de recolección de información, se volviera a asumir que en caso de vulneración de la Cuarta Enmienda, se impedirían tales actividades.[111]Del mismo modo, la carta de la inmunidad empezaba a jugarse en el sector de las telecomunicaciones.

Según la nueva enmienda a la Ley, tal como señaló un artículo de *The Wall Street Journal*,[112]los socios privados o empresariales que colaboraron con el Gobierno desde la perspectiva del

seguimiento electrónico entre el 11 de septiembre de 2001 y el 17 de enero de 2007, gozarían en materia de responsabilidad civil, de inmunidades y protecciones adicionales. Dicha colaboración aparecería amparada en la compleja y discutida Sección 702 de la Ley. Concretamente, fueron los senadores Ron Wyden y Mark Udall[113] los encargados de solicitar una revisión para estimar el número aproximado de civiles norteamericanos que han visto expuestos sus datos e identidades electrónicas debido a la cooperación de las corporaciones con el Gobierno.

La Sección 702 resulta pues la pieza central de la Ley *FISA* tras su último ajuste. En la misma, se recoge, según el senador Wyden, la posibilidad, en beneficio del Gobierno, de utilizar una Ley que se oriente a la plena monitorización, tanto extranjera como nacional, para vigilar y someter la privacidad de ciudadanos estadounidenses, algo que compara con el motivo de surgimiento en origen de la Cuarta Enmienda.[114]

110 *El Director de Inteligencia Nacional y el Fiscal General, pueden, por períodos de hasta un año autorizar la adquisición de información de inteligencia extranjera relativa a personas que razonablemente se cree que se encuentran fuera de los Estados Unidos, si el Director de Inteligencia Nacional y el Fiscal General determinan que: [...] ( 3 ) la adquisición implica la obtención de la información de inteligencia extranjera a partir o con la ayuda de un proveedor de servicios de comunicaciones, guardián, u otra persona (incluyendo cualquier funcionario, empleado, agente u otra persona) que tiene acceso a las comunicaciones , ya sea que se transmiten o mientras están almacenadas*.
Véase Public Law 55-110th Congress: *Protect America Act of 2007*, August 5, 2007, Sec. 105: "Additional Procedure For Authorizing Certain Acquisitions Concerning Persons Located Outside The United States", en: https://www.congress.gov/bill/110th-congress/senate-bill/1927/text/pl

111 Public Law 261-110th Congress: *FISA Amendments Act of 2008*, July 10, 2008, Title VII: Additional Procedures Regarding Certain Persons Outside the United States, Sec. 702: "Procedures For Targeting Certain Persons Outside The United States Other Than United States Persons", en: https://www.gpo.gov/fdsys/pkg/PLAW- 110publ261/html/PLAW-110publ261.htm

112 Tal como indica el artículo, los socios privados que actúan de acuerdo con las órdenes, certificaciones, o directivas previstas en la Ley deberán estar protegidos contra la responsabilidad futura. [...] La Ley establece normas y procedimientos para la protección de responsabilidad para los proveedores de servicios de comunicaciones electrónicas que ayudaron especialmente, cuando el *Terrorist Surveillance Program* estuvo actuando.
Véase "FISA Amendments Act of 2008", June 19, 2008, *The Wall Street Journal*, en: http://www.wsj.com/articles/SB121391360949290049

113 Committee Amendment Proposed by Mr. Wyden (For himself and Mr. Udall of Colorado): *Report on The Implementation Of The FISA Amendments Act of 2008*, June 2012, en: http://www.wired.com/images_blogs/dangerroom/2011/07/Secret-Law-Amendment-for-IA.pdf

114 *Esto suena a algo familiar, órdenes generales bajo la fórmula de la writ of assistance, que permitieron a los funcionarios del Gobierno decidir sobre el grado de privacidad a invadir, fueron exactamente el tipo de abuso hacia el que los colonos americanos protestaron, y que llevaron a los fundadores a adoptar la Cuarta Enmienda*. Véase WYDEN, Ron: *Prepared Remarks of Senator Ron Wyden on a Bill to Extend the FISA Amendments Act of 2008*, p. 7, en: http://www.wyden.senate.gov/

El peligro, por tanto ya no es que las corporaciones que cooperan con el Gobierno cedan los datos de sus clientes en manos de las Agencias de inteligencia, sin previo consentimiento de los mismos, sino que el aparato y la estructura, en un inicio orientados hacia amenazas ubicadas más allá de las fronteras nacionales sufre una distorsión y comienza a mirarse a sí mismo, convirtiendo a los propios civiles estadounidenses en probable amenaza a ojos de la vigilancia. Como indicó Wyden, en el Comité de Investigación sobre la *FISA Amendments Act* de 2008, la nueva Sección 702, no implicaba la mera obtención de registros individuales, sino que le permitía al Gobierno "*obtener órdenes programáticas que duran un año entero y le autorizan a recoger un número potencialmente elevado de llamadas telefónicas y mensajes de correo electrónico, sin necesidad de que los remitentes o destinatarios estén realmente conectados con el terrorismo o el espionaje*".[115]

**La Comprehensive National Cybersecurity Initiative. El acento de la ciberseguridad.** [2008]

En enero de 2008, la Administración Bush estableció la *Comprehensive National Cybersecurity Initiative* (*CNCI*), para fomentar un enfoque múltiple en la identificación de las emergentes amenazas cibernéticas,[116]apuntalar las telecomunicaciones actuales y futuras, y detectar las vulnerabilidades cibernéticas, con objeto de hacer frente de forma proactiva a las entidades que desean robar o manipular los datos protegidos en los sistemas federales de seguridad. Si bien los datos de las Agencias federales demuestran que la mayoría de ataques cibernéticos con éxito hasta la fecha, se han centrado en recursos de información virtuales, muchos expertos[117] consideran que la progresión de las intrusiones hace pensar en un ataque futuro a infraestructuras,[118]que permitan temporal o permanentemente, deshabilitar por ejemplo, la red de telecomunicaciones, el suministro de energía o el colapso económico.

No obstante, a pesar de la iniciativa, legisladores y analistas han expresado en varias ocasiones su preocupación acerca de que el marco legal actual aborde adecuadamente las amenazas de ciberseguridad modernas. En este sentido, el *Center for Strategic and International Studies* (*CSIS*), ha recomendado que las disposiciones federales sobre el ciber-crimen sean revisadas, en atención a una nueva legislación que elimine la distinción legal vigente entre las normas técnicas, para los sistemas nacionales de seguridad y las normas de los sistemas de agencias civiles y adoptar un enfoque basado en el riesgo a la seguridad informática federal.[119]

download/?id=b72ed3a0-fb8b-4e04-897b- d622de64c-d19&download=1

115 Ibíd.

116 Al igual que otros desafíos a la seguridad nacional en la era post 11-S, la amenaza cibernética es multifacética y carece de límites claramente delineados. Algunos atacantes cibernéticos operan a través de operaciones militares o de recogida de información de las Naciones extranjeras, mientras que otros tienen conexiones con grupos terroristas. Algunas amenazas informáticas incluso pueden proceder directamente de empresas criminales internacionales o nacionales.
Véase ROLLINS, John & HENNING, C. Anna: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, Congressional Research Service, CRS Report, March 10, 2009, p. 2, en: https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf

117 De hecho, expertos en seguridad nacional han hecho hincapié en la vulnerabilidad de las infraestructuras de Estados Unidos. En enero de 2009, el ex Director de Inteligencia Nacional, Mike McConnell, equiparaba "armas informáticas" con "armas de destrucción masiva", cuando expresó su preocupación por el "uso de los terroristas de la tecnología para degradar la infraestructura del país". Ibíd., p. 3.

118 El Departamento de Energía llevó a cabo un experimento en 2007 en el que el sistema de control de un generador sin conexión, que contenía componentes similares a la de los generadores más grandes conectados a muchas redes de energía que suministran electricidad a la nación, fue dañado y se convirtió en inoperable.
Ibíd.

119 Además, el marco legal actual, en particular la *Federal Information Security Management Act*, promulgada en 2002 para establecer las defensas de la Agencia contra las amenazas informáticas, resulta demasiado débil para prevenir con eficacia intrusiones cibernéticas.
Ibíd., p. 5.

Los legisladores hicieron algunos intentos por modernizar el marco legal existente en el 110 Congreso,[120]sin embargo, los analistas argumentan que, en última instancia, no hay cambio en el régimen legal existente que equipare adecuadamente a las agencias ejecutivas para prevenir ciberataques en los Estados Unidos.[121]

### 3.3.1.2. Escándalo revelado por USA Today. Cooperación entre la NSA y las compañías de telecomunicaciones: casos de AT&T, Verizon y BellSouth [Mayo-Junio 2006]

El 11 de mayo de 2006, la periodista del *USA Today*, Leslie Cauley, dio a conocer en plena vorágine de las primeras reformas a la Ley *FISA* y a la expectativa del posterior y último ajuste sobre la Sección 702 realizado en 2008; la cooperación entre las compañías *AT&T*, *Verizon* y *BellSouth* con la *NSA* para acceder en secreto a los registros telefónicos de millones de ciudadanos estadounidenses, bajo el titular: "*La NSA posee una base de datos masiva de llamadas telefónicas de estadounidenses*".[122]Con el empleo de unas fuentes de primer orden, que la periodista decidió no revelar, (se reconoce que son miembros cercanos al Gobierno), se mostró la intención de la Agencia de "*crear una base de datos que jamás se haya hecho dentro de las fronteras de la nación*", según confesaron alguno de los entrevistados.

De la misma manera, siempre según el planteamiento del artículo, las compañías mencionadas proporcionan la información a la Agencia, quien escucha y graba las conversaciones para analizar patrones de llamada en un esfuerzo por detectar la actividad terrorista, sin filtros ni distinciones, convirtiendo en sospechosos a la población en general. Valiéndose de la *Terrorist Surveillance Act,* el Presidente Bush habría autorizado unilateralmente a la *NSA*, sin intervención del Tribunal *FISA* en el proceso, a espiar las llamadas internacionales y los correos electrónicos de personas sospechosas de tener algún tipo de relación o nexo terrorista.

Tanto Don Weber, portavoz de la *NSA* ante los medios de comunicación, así como Dana Perino, subsecretaria de prensa de la Casa Blanca, se mostraron reticentes[123] ante estas informaciones y negaron la existencia de tal programa, aunque se confería la necesidad de abarcar cualquier ámbito que fuera imprescindible para acabar con el terrorismo de Al-Qaeda.

La cooperación de *AT&T* (en ese momento dirigida por C. Michael Armstrong), *Verizon* (encabezada por Ivan Seidenberg) y *BellSouth* (liderada por F. Duane Ackerman) en tanto que representan las tres mayores compañías de telecomunicaciones del país; garantizaba el acceso al servicio telefónico local e inalámbrico de más de 200 millones de clientes. Sin embargo, la *NSA* se topó con un problema, un agujero en su base de datos generado por la negativa a participar en el proyecto de *Qwest*. Aproximadamente 14 millones de clientes de esta compañía de telecomunicación quedaban al margen del espionaje de la Agencia, fundamentalmente por las dudas legales que a *Qwest* le parecía que trascendía

120 Por ejemplo, una enmienda de 2008 introducida en la *Federal Information Security Management Act* por iniciativa del Senador Carper, que habría añadido un cargo de Director de Seguridad como complemento al cargo de Director de Información, requerido en cada Agencia federal bajo la *Federal Information Security Management Act* de 2002 y la *ClingerCohen Act* de 1996.
Ibíd.

121 Argumentan que sólo la Casa Blanca tiene la autoridad y la supervisión necesaria para la seguridad cibernética.

122 CAULEY, Leslie. "NSA has massive database of Americans' phone calls", May 11, 2006, *USA Today*, en: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

123 Don Weber, portavoz de la *NSA*, se negó a discutir las operaciones de la Agencia: "teniendo en cuenta la naturaleza del trabajo que hacemos, sería irresponsable hacer comentarios sobre cuestiones operativas reales o supuestas, por lo tanto, no tenemos información que ofrecer" dijo. "Sin embargo, es importante señalar que la NSA toma en serio sus responsabilidades legales y opera dentro de la Ley". La Casa Blanca no quiso hablar sobre el programa: "no hay vigilancia doméstica sin autorización judicial", dijo Dana Perino, subsecretaria de prensa. inteligencia llevadas a cabo por el Gobierno federal "son lícitas y
necesarias para la persecución de Al-Qaeda y los terroristas afiliados". Ibíd.

del hecho de cooperar suministrando información de clientes sin orden judicial. La Orden Ejecutiva que presumiblemente firmara Bush valiéndose de su mayor autoridad en las tareas de inteligencia, resultaría el elemento clave al dotar de capacidad total a la *NSA* en la obtención de los datos. Algo que no sólo se contrapone con la Cuarta Enmienda, sino como indica bien Cauley, rechaza por completo la Sección 222[124] de la *Communications Act* aprobada y en vigor desde 1934.[125]

Por su parte, las corporaciones suministradoras, también negaron la colaboración con la *NSA*,[126]en un ejercicio que recordaba a los esfuerzos de los portavoces de *RCA Global*, *ITT World Communications* y *Western Union International* de eludir su implicación en el programa *SHAMROCK*, hacía ya más de 30 años antes.

Añadió que todas las actividades nacionales de En una información posterior del *USA Today*, concretamente del 30 de junio,[127]la propia Cauley en colaboración con los también periodistas John Diamond, Jim Drinkard, Peter Eisler, Thomas Frank, Kevin Johnson y Susan Page desvelaron que los propios miembros del Congreso y del Senado[128] norteamericano conocían de la existencia de la base de datos de la *NSA* del mismo modo que las fuentes conferían credibilidad a las informaciones que involucraban a las empresas *AT&T*, *Verizon* y *BellSouth* con el programa de suministro masivo de datos a la *NSA*.

En una declaración[129] en respuesta a estas nuevas acusaciones, *Verizon* sembró definitivamente las dudas cuando se negó a calificar las informaciones de verdad o mentira alegando que el programa de cooperación existía pero que el carácter altamente clasificado del mismo hacía imposible cualquier revelación. La declaración significó un paso en falso en las expectativas de mantener en secreto el proyecto, dado que multitud de medios[130] comenzaron a tirar

124 *Cada operador de telecomunicaciones tiene el deber de proteger la confidencialidad de la información de propiedad de, y en relación con, otros operadores de telecomunicaciones, fabricantes de equipos, y los clientes*. Senate and House of Representatives of the United States of America in Congress assembled: *Communications Act of 1934*, Title II: Common Carriers, Sec. 222: "Privacy of Customer Information", June 1934, p. 52, en: https://transition.fcc.gov/Reports/1934new.pdf

125 Bajo la Sección 222 de la *Telecommunications Act* de 1996, (aprobada sobre la base del texto de 1934), las compañías telefónicas tienen prohibido ofrecer información sobre hábitos de llamadas de sus clientes: los registros de las personas a las que se llama y el tiempo de duración, llamadas entrantes así como las llamadas inalámbricas, que también están protegidas. Las sanciones económicas por violar la Sección 222, uno de los muchos refuerzos de privacidad que se han agregado a la Ley en los últimos años, pueden ser fuertes. La Comisión Federal de Comunicaciones, organismo regulador de las telecomunicaciones de la nación, puede imponer multas de hasta 130.000 dólares por día de violación, con un tope de 1.325 millones de dólares por violación Cauley, "NSA has massive database", op. cit..

126 Cuando se le preguntó sobre el programa a *AT&T*, esta respondió con un comentario a *USA Today*: "no hacemos comentarios sobre asuntos de seguridad nacional, excepto para decir que sólo ayudamos a los organismos encargados de hacer cumplir la protección de la seguridad nacional". En otro comentario, *BellSouth* dijo: "*BellSouth* no proporciona ninguna información confidencial de los clientes a la NSA o cualquier Agencia gubernamental sin autorización legal adecuada". Por su parte, *Verizon*, la compañía de telecomunicaciones nº 2 de los EE.UU. por detrás de *AT&T*, dio esta declaración: "no hacemos comentarios sobre asuntos de seguridad nacional, actuamos en plena conformidad con la Ley y estamos comprometidos a salvaguardar la privacidad de nuestros clientes".

127 CAULEY, Leslie., DIAMOND, John., DRINKARD, Jim., EISLER, Peter., FRANK, Thomas., JOHNSON, Kevin., et al. "Lawmakers: NSA database incomplete", June 30, 2006, *USA Today*, en: http://usatoday30.usatoday.com/news/washington/2006-06-30-nsa_x.htm

128 Diecinueve legisladores que habían sido informados sobre el programa, verificaron que la *NSA* ha construido una base de datos que incluye los registros de las llamadas telefónicas nacionales estadounidenses. Según sus declaraciones, el programa incluye los registros de los números marcados y la duración de las llamadas, pero no implican la escucha de las llamadas o la grabación de su contenido.
Ibíd.

129 "El Presidente se ha referido a un programa de la NSA que él mismo autorizó y dirigió contra Al-Qaeda", dijo *Verizon* en una declaración escrita el 12 de mayo. "Debido a que el programa es altamente clasificado, Verizon no puede hacer comentarios sobre ese programa, ni podemos confirmar o negar si hemos tenido alguna relación con él", sentenció.

130 Por ejemplo, *The New York Times* informó el 12 de mayo que un alto funcionario del Gobierno había confirmado que la *NSA* tenía acceso a los registros de la mayoría de las llamadas telefónicas en los EEUU, pero

del hilo y acabaría por demostrarse un planteamiento de vigilancia masiva confirmado posteriormente con la entrada en escena de Edward Snowden.

### 3.3.2. Administración Barack Obama. [2009-Actualidad]

#### 3.3.2.1. El escándalo Verizon y el doble discurso de Barack Obama.

Con el legado de un sistema empoderado, apoyado en una mayor autonomía presidencial y sustentado en el temor que causó el pensamiento de repetir los acontecimientos del 11-S, Barack Obama se convertía en el cuadragésimo cuarto Presidente de los Estados Unidos de América.

Los esfuerzos de Obama en materia de inteligencia, tienen un antes y un después en el año 2013, tras las manifestaciones del ex contratista de la *NSA*, Edward Snowden (en el mes de mayo), que sacaba a la luz los excesos y abusos de poder en la obtención de material por la Agencia. Así,

Obama tuvo que enfrentar las acusaciones de *The New York Times* acerca de la existencia durante su primera Administración de "*un programa de vigilancia doméstica en el que se compilan los registros comerciales de telecomunicaciones que involucran a los estadounidenses*", tal como recogían los periodistas Charlie Savage y Edward Wyatt.[131]

Para poder acceder a tales cantidades de información confidencial el Gobierno habría implementado su autoridad sobre el Tribunal *FISA*. Mediante Orden judicial firmada por el juez Roger Vinson en julio,[132]se obligaba a *Verizon* a facilitar las copias electrónicas de "*todos los registros detallados de llamadas o metadatos de telefonía creados por Verizon para las comunicaciones entre los Estados Unidos y en el extranjero o totalmente dentro de los Estados Unidos, incluyendo llamadas telefónicas locales*". La orden fue catalogada como *TOP SECRET*, es decir, prohibiendo expresamente a *Verizon* su revelación pues se trataba de una información de grado sensible que no podía darse a conocer antes de la fecha de desclasificación del material, fijada en la propia orden para no antes del año 2038.

Entre las informaciones a suministrar se incluyen, la "*información de la sesión de identificación, los números de origen y número de terminación, la duración de cada llamada, teléfono de tarjeta de llamada, Identidad del número internacional del abonado móvil, y la información integral de enrutamiento*".[133]

Durante su carrera como candidato en oposición a Bush, una de las proclamas del hoy Presidente norteamericano fue su convencida lucha contra lo que su propio gabinete se encargó en denominar la "*guerra de la vigilancia*". No obstante, esa guerra en favor de la campaña electoral y en un terreno de reivindicación de la privacidad civil, contrasta con el Obama Presidente, mucho más pragmático, tratando de dar continuidad al atajo de laberintos legales de la Administración Bush y procurando, "*bloquear cualquier decisión judicial contra hechos que evadieran la Ley en la Administración anterior. También, buscando con cierto éxito invocar la doctrina del secreto de Estado para evitar cualquier revisión judicial de acciones potencialmente criminales en la era Bush*", como señalaba el diario *The Guardian*[134] tras

dijo que los registros se utilizan de manera limitada para realizar un seguimiento. *The Washington post* informó el mismo 12 de mayo que fuentes con conocimiento del programa informaron que la Administración Bush había recogido los registros telefónicos domésticos en bases de datos enormes y que las empresas que cooperaron con la *NSA* permiten mayor registro debido al dominio del mercado de las telecomunicaciones de Estados Unidos y la conexión de cientos de miles de millones de llamadas telefónicas cada año.

131 SAVAGE, Charlie & WYATT, Edward. "U.S. Is Secretly Collecting Records of Verizon Calls", June 5, 2013, *The New York Times*, en: http://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html

132 United States Foreign Intelligence Surveillance Court: *Full order Roger Vinson*, Washington D.C., July 19, 2013, en: http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

133 Ibíd., p. 2.

134 SEYMOUR, Richard. "Obama's Verizon phone records collection carries on Bush's work", June 6, 2013, *The Guardian*, en: http://www.theguardian.com/commentis-

el pleno conocimiento de las prácticas del Gobierno con la compañía *Verizon*.

En cualquier caso, el documento del Juez Vinson, supone la primera demostración pública de que bajo el Gobierno de Obama se continuaba la senda marcada por Bush en materia de recogida de registros telefónicos de millones de ciudadanos estadounidenses sin importar la mediación de sospechas o delitos, como llegó a indicar *The New York Times*, la prueba de que "*Obama está demostrando la necedad de que el Poder Ejecutivo utilizará cualquier instrumento que se otorga y muy probablemente el abuso*".[135]

La necesidad de hacer frente a las acusaciones apremió al Presidente a la comparecencia pública del 17 de enero de 2014, donde hizo balance del Estado de vigilancia y asumió su cambio de conciencia con relación a su discurso de campaña electoral. Concibiendo que en el afán de responder a las posibles amenazas globales, el riesgo de extralimitación del Gobierno y por ende, la posibilidad de privación de libertades aumentaba,[136]Obama quiso recuperar su pensamiento crítico con la inteligencia antes de llegar a la Casa Blanca, denotándolo de "*sano escepticismo*"[137]hacia los programas de vigilancia, insistiendo en las reformas que pretendía implementar en las Agencias y la decisión prioritaria de no disolver los programas dado que a su juicio, no violaban la Ley ni demostraban arrogancia alguna sobre la libertad civil.[138]La negativa a desarmar "*unilateralmente*" las Agencias de inteligencia se fundamentaba en el espionaje internacional, algo que Obama en su discurso reflejó tratando de dar a entender que constantemente diversas células se hallaban investigando nuevas vías para conseguir interceptar o erosionar las redes gubernamentales y del sector privado norteamericano accediendo a los correos electrónicos y comprometiendo los sistemas.[139]

Apostando por un mayor ejercicio de transparencia,[140]y reconociendo que se hace necesario ofrecer una protección adicional a la práctica de la Sección 702 de la Ley *FISA*,[141]Obama procedió a

free/2013/jun/06/obama-verizon-phone-records-bush

135 Editorial board: "President Obama's Dragnet", June 6, 2013, *The New York Times*, en: http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=1&_r=2

136 *En nuestra prisa por hacer frente a una nueva serie de amenazas muy reales, el riesgo de un exceso por parte del Gobierno —la posibilidad de perder algunas de nuestras libertades esenciales en pos de la seguridad—, también se han visto pronunciadas. Hemos visto que, inmediatamente después del 11 de septiembre, nuestro Gobierno se dedicó a implementar técnicas de interrogación perfeccionadas que contradecían nuestros valores. Cuando era senador, sostuve una postura crítica respecto de diversas prácticas, como las escuchas telefónicas sin orden judicial. Con demasiada frecuencia, se instituían nuevas autoridades sin el debate público que merecían.*
*President Obama's Full NSA Speech*, January 17, 2014, 06:02-06:43, en: https://www.youtube.com/watch?v=p4MK-m2uFqVQ

137 *Por todos estos motivos, mantuve un sano escepticismo en relación con nuestros programas de vigilancia después de convertirme en Presidente. Ordené que mi equipo de seguridad nacional y nuestros abogados revisaran nuestros programas, y en algunos casos ordené que se hicieran cambios en la forma en que desempeñábamos nuestras actividades. Aumentamos las tareas de supervisión y auditoría, e incluimos nuevas estructuras enfocadas al cumplimiento. El Gobierno propuso normas mejoradas, que recibieron la aprobación del Tribunal de Vigilancia de Inteligencia Extranjera. Y nos esforzamos por mantener al Congreso informado en todo momento en relación con estas actividades.*
Ibíd., 09:49-10:23.

138 *Lo que no hice es detener estos programas por completo, no solo porque consideraba que nos protegían, sino también porque no había nada en ese análisis inicial, y nada de lo que me haya enterado desde entonces, que indicara que nuestra comunidad de inteligencia hubiera intentado infringir la Ley o ignorar las libertadas civiles de sus conciudadanos.*
Ibíd., 10:25-10:48.

139 *Existe una razón por la cual los teléfonos BlackBerry o iPhones no están permitidos en la Sala de situaciones de la Casa Blanca. Sabemos que los servicios de inteligencia de otros países —incluidos algunos que fingieron sorprenderse por las divulgaciones de Snowden— están constantemente sondeando nuestras redes del Gobierno y del sector privado, y acelerando la elaboración de programas para escuchar nuestras conversaciones, interceptar nuestros mensajes de correo electrónico y comprometer nuestros sistemas.*
Ibíd., 17:23-17:48.

140 *Realizaremos reformas de los programas y procedimientos en vigor para proporcionar mayor transparencia a nuestras actividades de vigilancia y para fortalecer las salvaguardias que protegen la privacidad de los ciudadanos estadounidenses.*
Ibíd., 22:21-22:32.

141 *Proporcionaremos protecciones adicionales para las actividades realizadas en virtud de la Sección 702, la cual permite que el Gobierno intercepte las comunicaciones de objetivos extranjeros en el exterior que tengan información importante para nuestra seguridad nacional. En concreto, le he pedido al*

utilizar lo que su predecesor en el cargo hizo tantas veces con anterioridad, defender la Sección 215 de la Ley Patriótica con el ahínco de la amenaza terrorista, al negar que la *NSA* haga un uso ilícito de los datos recopilados en la base de datos, y reconociendo que la utilidad radica simplemente en el fin de "*otorgar una ventaja específica frente a la amenaza*".[142]Del mismo modo, Obama reconoció que la inteligencia norteamericana no se halla ejerciendo su actividad secreta para "*suprimir la crítica o la disidencia*", ni atendiendo en base a filtros como pudieran ser el origen étnico o la creencia religiosa del individuo, así como negó la recopilación sometida a ventajas competitivas en beneficio de empresas o corporaciones estadounidenses.[143]

Finalmente, Obama en nombre de la comunidad de inteligencia determinó en el final de su discurso la necesidad de no pedir disculpas[144] por lo que cree, es una actividad extendida al resto de países del mundo, y el perdón no tiene sentido solicitarlo cuando de la búsqueda de una mayor eficiencia se trata. En todo caso, las promesas de las reformas no adquirieron el calado que parecía buscar el Presidente, a quien la ambivalencia en el discurso con relación a la comunidad de inteligencia, antes y durante la presidencia han parecido desgastarle en los medios de comunicación. Así, tras su comparecencia, algunos medios como *The Guardian*, acusaban la táctica de "*estafa reconocible*",[145]como indicó el periodista Glenn Greenwald, el mismo que se reunió con Edward Snowden y a quien el ex analista confirió la responsabilidad de dar a conocer al público los excesos de vigilancia de la *NSA*.

#### 3.3.2.2. El papel del United States Foreign Intelligence Surveillance Court. Seguridad o derechos.

Uno de los instrumentos encargados de regular las actividades de inteligencia depurando los posibles abusos y manteniendo a raya los excesos cuando se produjesen, es el Tribunal *FISA*, de Vigilancia de Inteligencia Extranjera de los Estados Unidos. Su origen respondió a una estructura judicial capaz de filtrar mediante ordenaciones, conocidas como órdenes *FISA*, las tareas de las Agencias. De esta manera, si una Agencia de inteligencia quería acometer actos de vigilancia debía solicitar previamente la autorización al Tribunal, quien tras considerar las posibles vulneraciones o por el contrario, la no invasión en el terreno privado del individuo o grupo objetivo, decidiría omitir u otorgar el permiso.

---

*Secretario de Justicia y al Director Nacional de Inteligencia que lleven a cabo reformas que impongan limitaciones adicionales a la capacidad del Gobierno de conservar, buscar y utilizar en casos penales las comunicaciones entre ciudadanos estadounidenses y ciudadanos extranjeros que se hayan recopilado incidentemente en virtud de la Sección 702.*
Ibíd., 23:45-24:19.

142 *El programa de metadatos telefónicos en virtud de la Sección 215 se concibió con el propósito de detectar la procedencia de las comunicaciones de terroristas, para que podamos ver, con la mayor rapidez posible, con quiénes pueden estar en contacto. Y esta capacidad también podría resultar valiosa ante una crisis. Por ejemplo, si estalla una bomba en una de nuestras ciudades y las fuerzas del orden público están intentando determinar contra reloj si hay una red que está a punto de perpetrar ataques adicionales, cada segundo cuenta.*
Ibíd., 26:49-28:10.

143 *También he dejado bien claro que Estados Unidos no recopila datos de inteligencia con el fin de suprimir las críticas o la disidencia, ni tampoco recopilamos inteligencia para poner en situación de desventaja a las personas en función de su origen étnico, raza, género, orientación sexual o convicciones religiosas. Tampoco recopilamos inteligencia para proporcionar una ventaja competitiva a empresas estadounidenses o sectores comerciales estadounidenses.*
Ibíd., 34:51 - 35:14.

144 *Nuestras agencias de inteligencia continuarán recopilando información sobre las intenciones de Gobiernos —y no de los ciudadanos comunes— en todo el mundo, de la misma manera que hacen los servicios de inteligencia de todos los países. No pediremos disculpas por el simple hecho de que nuestros servicios sean más eficaces. Pero los Jefes de Estado y los Gobiernos con los que trabajamos de cerca, y de cuya cooperación dependemos, deben tener la confianza de que los tratamos como verdaderos socios. Y los cambios que he ordenado son precisamente para eso.*
Ibíd., 37:07-37:43.

145 *En última instancia, la esencia de la NSA perdurará totalmente incluso si todas las propuestas de Obama son adoptadas.* [...] *En otras palabras, el objetivo no es reformar verdaderamente la Agencia; se trata más bien de engañar a la gente para que crea que ya no deben temer o molestarse acerca de la vigilancia.*
Véase GREENWALD, Glenn. "Obama's NSA 'reforms' are little more than a PR attempt to mollify the public", January 17, 2014, *The Guardian*, en: http://www.theguardian.com/commentisfree/2014/jan/17/obama-nsa-reforms- bulk-surveillance-remains

No obstante, resulta sencillo imaginar que si la propia Ley *FISA* que creó el sistema de Tribunales en el mismo instante histórico y con el parecido propósito ha sido "*reajustada*" especialmente en las dos últimas Administraciones presidenciales, los Tribunales sujetos a la propia Ley, del mismo modo, han sufrido la mediatización gubernamental, algo que en este caso puntual no está tan intrínsecamente ligado a los últimos tiempos, sino desde su propio origen en octubre de 1978. Más allá de la polémica surgida en 2013 ya abordada, con el conocimiento público de la orden del juez Vinson; el Tribunal *FISA*, con el paso de los años ha aseverado el control del Gobierno a la vigilancia de las comunicaciones. El propio Presidente del Tribunal, el juez por el Distrito de Columbia, Reggie B. Walton, ha dejado caer en varias ocasiones el "*beneficio potencial de informar mejor al público sobre las decisiones de la Corte*".[146]Sin embargo, reconoce los obstáculos que hay para hacerlo debido a los múltiples malentendidos por la omisión de datos, dada la naturaleza secreta del Tribunal.

Según *EPIC.org* (*Electronic Privacy Information Center*)[147]la compilación del número de órdenes presentadas al Tribunal *FISA*, así como las aprobadas, modificadas o rechazadas por el mismo, entre 1979 y 2013, denotan la dependencia absoluta y el servilismo en la actuación del Tribunal, que lejos de constituirse como el filtro como el que nació, dota al Gobierno de la impunidad a la hora de acometer actos de vigilancia, doméstica e internacional. Veamos en la siguiente tabla esta proyección de *EPIC.org* sobre las órdenes *FISA* y la actuación del Tribunal.

Como se puede observar, el Tribunal de Vigilancia de Inteligencia Extranjera durante treinta y cuatro años de actividad aprobó la mayoría de las solicitudes presentadas por las Agencias de inteligencia. Es importante tener en cuenta que hay años naturales donde el número de peticiones al Tribunal es inferior a las solicitudes aprobadas, y años en que ese mismo número es superior. En el primer caso, esto se explica por aquéllas posibles solicitudes que se pierden en el camino debido a un defecto de forma en su redacción o planteamiento. En el segundo, se debe a la proactividad del Tribunal, quien también es competente para iniciar el mandato de vigilancia a un objetivo.

De este modo, apenas 12 órdenes de un total de 35.333 durante el período de actividad 1979-2013 fueron rechazadas por los jueces del Tribunal *FISA*. Del mismo modo, en la proyección de los datos se observa la frecuencia al alza de la emisión y aprobación de órdenes con el comienzo del nuevo siglo, en el año 2000, lo que vendría a confirmar, que a pesar de los errores sobre todo internos en la colaboración entre las Agencias, la actividad y la sospecha se había disparado desde un año antes de los atentados del 11-S.

#### 3.3.2.3. Obstáculos en la reforma para limitar las funciones de la NSA. [18 noviembre 2014]

Después de anunciar las reformas necesarias en su discurso a principios de año, el Presidente Obama parecía tener clara la necesidad de emprender una reforma de los sistemas de vigilancia, de las prácticas al amparo de la Sección 702 y ante todo de los programas desarrollados por la *NSA*. Con ese propósito en junio de 2014 la Administración Obama impulsó el Proyecto de Ley *USA FREEDOM ACT*.[148]En el comienzo del documento se dejó claro que el propósito no era otro que determinar la autoridad del Gobierno Federal a la hora de "*exigir la producción de ciertos registros de negocios, llevar a cabo la vigi-*

146 LICHTBLAU, Eric. "In Secret, Court Vastly Broadens Powers of N.S.A", July 6, 2013, *The New York Times*, en: http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of- nsa.html?nl=todays-headlines&emc=edit_th_20130707&_r=0

147 *EPIC* es un centro de investigación independiente sin fines de lucro ubicado en Washington D.C. Trabaja para proteger la privacidad, la libertad de expresión, los valores democráticos y la promoción de la voz pública en las decisiones sobre el futuro de Internet.

148 También conocida como: *Uniting And Strengthening America By Fulfilling Rights And Ensuring Effective Discipline Over Monitoring Act of 2015*.

*lancia electrónica, rastreo de dispositivos y utilizar otras formas de recolección de información para la inteligencia extranjera, contraterrorismo, con fines delictivos y para otros fines*".[149]

Aunque desde el ámbito puramente jurídico la *USA FREEDOM ACT* no supone un gran progreso en el cambio de las actividades de la comunidad de inteligencia, sí deja la puerta abierta a un uso más restrictivo de la Sección 702 en manos de los servicios de inteligencia. De esta manera, se incide en que cualquier información obtenida de forma irregular o vulnerando derechos civiles, catalogada como deficiente por el Tribunal *FISA*, no podrá ser utilizada o revelada por ninguno de los actores involucrados en la investigación pertinente, excepto cuando la Fiscalía General decrete la autorización debido a una posible amenaza de muerte o lesiones graves que pudieran causarse a una persona.

Esto sin duda, limitaba las capacidades de la *NSA* a la hora de solicitar registros telefónicos a las compañías, algo que sólo podría ejecutar en caso de pruebas razonables acerca de los individuos investigados. Por ende, las corporaciones empresariales, como *Apple*, *Google*, *Microsoft* y *Yahoo*, que siempre habían percibido como un juego dudoso la actitud del Estado respecto a los registros de sus clientes, observaban cómo el nuevo Proyecto de Ley les favorecía al no actuar fuera de la Ley, sólo suministrando los datos de aquéllas personas o grupos realmente sospechosos de actividades delictivas.

Tras las elecciones al Congreso de 2014, y un debate acalorado sobre el nuevo Proyecto, el Senado votó el 18 de noviembre la reforma de la comunidad de inteligencia, con la idea de quebrar los excesos de la *NSA*. A pesar del gran apoyo demócrata a la Ley, con 54 votos a favor, a los que se adhirieron 4 republicanos, al no lograr reunir los 60 votos necesarios y con la oposición de 42 votos en contra, entre los cuáles 41 procedían del ala republicana de la cámara, la reforma no salió adelante. Fundamentalmente, la amenaza terrorista representada por el mal llamado Estado Islámico fue el motivo[150] por el que el sector republicano, según el senador Mitch McConnell, decidió votar en contra de debilitar el sistema de inteligencia o al menos, de hacerlo más liviano. Por su parte, el senador Patrick Leahy, quien redactó el Proyecto, lamentó[151] el resultado entendiendo que el alarmismo opositor había resultado el vencedor.

Así pues, el intento de reforma se topó de bruces con el bloqueo parlamentario.

#### 3.3.2.4. La sustitución de la USA PATRIOT ACT de 2001 por la USA FREEDOM ACT [31 de mayo 2015]. ¿Triunfo de Snowden o argucia política?

Con el rechazo aún latente y con el mismo propósito de reforma, la *USA FREEDOM ACT* tuvo su segunda oportunidad en abril de 2015, momento en que fue de nuevo tramitada al Comité judicial del Senado.

El recorrido de la Ley cabe entenderlo en un doble contexto. Por un lado, la hemorragia que suponían las revelaciones de Edward Snowden sobre los programas de vigilancia de la *NSA*, desde que decidiera contar los entresijos del programa *PRISM* en junio de 2013 al diario *The Guardian*. Por el otro, la expiración de la *USA PATRIOT ACT*, creada para ser útil hasta el 1 de junio de 2015.

De esta manera, el nuevo proyecto se planteó al Senado, y a pesar de las reticencias y el voto en

149 113th Congress: *USA FREEDOM ACT of 2014*, June 5, 2014, en: http://www.leahy.senate.gov/imo/media/doc/HEN14602.pdf

150 Sobre el fracaso en el intento de reformar la comunidad de inteligencia para impedir los abusos de los programas de la *NSA*, McConnell dijo: "este es el peor momento posible para tener las manos atadas a la espalda".

151 Patrick Leahy, Presidente demócrata del Comité Judicial del Senado y uno de los patrocinadores del Proyecto de Ley, acusó "a los críticos de usar tácticas alarmistas sobre ISIS y otras amenazas terroristas". "Fomentando el temor se ahoga el debate serio y las soluciones constructivas", terminó.
Véase DYER, Geoff: "US Republicans face NSA dilemma", US Politics & Policy, November 19, 2014, *Financial Times*, en: http://www.ft.com/cms/s/0/68ad903c-6fa9-11e4-90af-00144feabdc0.html#axzz3itUj7h44

| EL PAPEL VIGILANTE DEL TRIBUNAL FISA [1979 – 2013] | | | | |
|---|---|---|---|---|
| Año | Número de solicitudes presentadas al Tribunal FISA | Número de solicitudes aprobadas por el Tribunal FISA | Número de solicitudes modificadas por el Tribunal FISA | Número de solicitudes rechazadas por el Tribunal FISA |
| 1979 | 199 | 207 | 0 | 0 |
| 1980 | 319 | 322 | 1 | 0 |
| 1981 | 431 | 433 | 0 | 0 |
| 1982 | 473 | 475 | 0 | 0 |
| 1983 | 549 | 549 | 0 | 0 |
| 1984 | 635 | 635 | 0 | 0 |
| 1985 | 587 | 587 | 0 | 0 |
| 1986 | 573 | 573 | 0 | 0 |
| 1987 | 512 | 512 | 0 | 0 |
| 1988 | 534 | 534 | 0 | 0 |
| 1989 | 546 | 546 | 0 | 0 |
| 1990 | 595 | 595 | 0 | 0 |
| 1991 | 593 | 593 | 0 | 0 |
| 1992 | 484 | 484 | 0 | 0 |
| 1993 | 509 | 509 | 0 | 0 |
| 1994 | 576 | 576 | 0 | 0 |
| 1995 | 697 | 697 | 0 | 0 |
| 1996 | 839 | 839 | 0 | 0 |
| 1997 | 749 | 748 | 0 | 0 |
| 1998 | 796 | 796 | 0 | 0 |
| 1999 | 886 | 880 | 0 | 0 |
| 2000 | 1005 | 1012 | 0 | 0 |
| 2001 | 932 | 934 | 4 | 0 |
| 2002 | 1228 | 1228 | 0 | 0 |
| 2003 | 1727 | 1724 | 79 | 4 |
| 2004 | 1758 | 1754 | 94 | 0 |
| 2005 | 2074 | 2072 | 61 | 0 |
| 2006 | 2181 | 2176 | 73 | 1 |
| 2007 | 2371 | 2370 | 86 | 4 |
| 2008 | 2082 | 2083 | 2 | 1 |
| 2009 | 1329 | 1320 | 14 | 2 |
| 2010 | 1511 | 1506 | 14 | 0 |
| 2011 | 1676 | 1789 | 30 | 0 |
| 2012 | 1789 | 1788 | 40 | 0 |
| 2013 | 1588 | 1588 | 34 | 0 |

* Fuente: Electronic Privacy Information Center.

contra del 22 de mayo de 2015 (57 a favor por 42 en contra), el 31 de mayo (con 77 votos a favor y 17 en contra) el Senado confería luz verde a la nueva Ley, que automáticamente, un día antes de expirar la *USA PATRIOT ACT* entraría en vigor, sustituyendo las prácticas de aquélla.

A pesar de contar con el apoyo de las compañías tecnológicas y de comunicaciones, así como del respaldo presidencial y aseverar un fortalecimiento de la privacidad, la nueva Ley quedó eclipsada por la noticia de la desaparición de su predecesora. Desde la perspectiva jurídica, aunque la *USA FREEDOM ACT* mantiene el espíritu de su primer planteamiento en noviembre de 2014, cabe entender que las diferencias son palpables.

De hecho, el *Center For Democracy and Technology (CDT)* es uno de tantos agentes que se mostraba a favor de la nueva Ley, pero al mismo tiempo rechazaba la versión de 2014. Llegados a este punto entonces hay que plantear la cuestión de las verdaderas diferencias entre ambos documentos legales. El propio *CDT* ha elaborado un documento[152] donde se escenifican los cambios más relevantes en relación a la polémica Sección 702, el papel del Tribunal *FISA* o la expiración de la Sección 215.

Podría creerse con facilidad que el triunfo de la *USA FREEDOM ACT*, actualmente en vigor, se debe a la presión ejercida por Snowden con sus revelaciones sobre las prácticas excesivas de la *NSA* en materia de vigilancia. No obstante, dada la coincidencia temporal de aprobación y la característica sustitutiva de la nueva Ley es importante entender que estamos ante una argucia política para aprovechar la polémica arrastrada por la *USA PATRIOT ACT* durante diez años y sacudir la polvareda al amparo de un nuevo documento que parece reescribir la historia desde cero.

A pesar de ligeras aportaciones positivas, como permitir que las empresas o personas reclamadas al efecto que fueran vigiladas por orden previa, puedan hacer pública la misma sin prohibición alguna, el hecho de que el Gobierno no esté firmemente requerido a dar explicaciones sobre el grueso de población investigada bajo la Sección 215 durante algo más de una década de la *USA PATRIOT ACT* o el número oficial de individuos investigados al amparo de la Sección 702 de la enmendada Ley *FISA*, resta naturaleza de cambio y dota de continuismo a la política de vigilancia liderada por la *NSA* en la actualidad.

## 4. El desafío de las filtraciones en la comunidad de inteligencia norteamericana.

### 4.1. Filtradores y filtraciones anteriores a WikiLeaks.

En la historia de la comunidad de inteligencia norteamericana son recurrentes, casi podríamos decir que desde sus orígenes, los casos de filtración de información secreta o el surgimiento, como fuentes de oposición, de antiguos analistas o colaboradores de las Agencias de inteligencia estadounidense que deciden mostrar públicamente su disconformidad con las prácticas gubernamentales.

Como punto de partida citaremos el caso de John Anthony Walker Jr, quien aún hoy está considerado como el mayor filtrador de documentos clasificados vinculantes a la Marina norteamericana. Ingresó en la Marina en 1956, como *radioman* y tras una impresión favorable de sus superiores, ascendió rápidamente.[153]Después de ser asignado a diferentes misiones en submarinos como el *USS Razorback* (*SS-394*), un submarino diésel de la Segunda Guerra Mundial o el *USS Andrew Jackson* (*SSBN-*

152 Center For Democracy and Technology (*CDT*), *Comparison of 2014 and 2015 versions of the USA FREEDOM ACT,* April 28, 2015, en: https://cdt.org/insight/comparison-of-2014-and-2015-versions-of-the-usa-freedom-act/

153 HEATH, J. Laura: *An analysis of the systemic security weaknesses of the U.S. Navy fleet broadcasting system, 1967-1974, as exploited by CWO John Walker*, M.S., Georgia Institute of Technology, Fort Leavenworth, Kansas, 2001, p. 10.

*619*),[154]en noviembre de 1967 fue reasignado como suboficial de guardia en la *Naval Communications Area Master Station* (estación central de comunicaciones de la flota submarina). A partir del año siguiente,[155]Walker ya había comenzado a colaborar con la inteligencia soviética[156] transmitiendo información clasificada, incluyendo libros de códigos e informes sobre los movimientos de submarinos y buques de guerra norteamericanos.[157]

Otro de los casos más relevantes de filtración de secretos de inteligencia fue el protagonizado por Daniel Ellsberg, cuya vida cambió por completo entre los años 1964 y 1971, en plena Guerra de Vietnam. Después de realizar tareas de analista estratégico militar en el Pentágono,[158]a la vuelta de su servicio en Vietnam, el Secretario de Defensa Robert S. McNamara, le encargó que colaborara en la redacción de un estudio[159] clasificado de alto secreto sobre la gestión de la Guerra. Estos documentos serán los conocidos como *Pentagon Papers*, los mismos que el propio Ellsberg entregó al diario *The New York Times* en el año 1971.[160]

Tal como señala Carlos Sánchez Hernández, la magnitud del cuarto poder que significó la prensa libre en el escándalo *Watergate* es imposible entenderla sin la filtración de los *Pentagon Papers* por Ellsberg, algo que provocaría un enorme terremoto político en Washington por el que su protagonista no sólo pasaría de héroe nacional al hombre más peligroso de América,[161]sino que significaría "*el comienzo de la caída imparable de Nixon así como la aceleración de la ya iniciada retirada estadounidense de Vietnam erosionando aún más la ya pésima imagen que la guerra tenía entre los norteamericanos para 1971*".[162]

Ellsberg fue acusado de dos cargos de robo y espionaje el 30 de junio de 1971, no obstante, el juez de la causa, Mateo Byrne, al contemplar varios

154 Uno de los primeros submarinos de misiles balísticos de propulsión nuclear.

155 Hacia 1967, los Walker estaban al borde de la quiebra, después de un negocio fallido, con lo que la oportunidad de ganar dinero fue la motivación por la que John decidió cooperar con la inteligencia soviética. El propio John llegaría a afirmar que le pagaban 4.000 dólares al mes por el robo de secretos de la *NAVCAMS*, un incremento exponencial si tenemos en cuenta que su sueldo como suboficial era de 725 dólares mensuales.
Véase Heath: *An analysis of the systemic security*, op. cit., p. 12.

156 No era el primer caso de colaboración con la URSS en plena escalada de la Guerra Fría. En 1953, con el trasfondo de la Guerra de Corea, el matrimonio Rosenberg (Julius y Ethel), fue acusado de suministrar información clasificada a agentes del Gobierno soviético. Tras aplicarse la Ley de Espionaje de 1917, fueron ejecutados en la silla eléctrica, en la que es, la primera ejecución de esta naturaleza por motivo de espionaje, en la historia de Estados Unidos.

157 Fue un soplo de Bárbara Walker, su ex mujer, el que hizo al *FBI* comenzar a seguir la pista de John, hasta que en 1985, se destapa la red de espionaje y extracción de información. El 6 de noviembre de 1986, John Walker fue condenado a dos cadenas perpetuas.

158 En 1964 comenzó a trabajar en una institución de investigación patrocinada por las Fuerzas Armadas, la *Rand Corporation*, donde destacó como teórico y analista, y en donde se fijó en él un alto funcionario del Departamento de Defensa, John McNauthon, ayudante directo del Secretario de Defensa, Robert S. McNamara. McNauthon le ofreció incluirlo en su equipo en el Pentágono, donde comenzaría a trabajar desde agosto de 1964.
Véase SÁNCHEZ HERNÁNDEZ, Carlos: "Analogías de la historia I: Julian Assange y Wikileaks vs Daniel Ellsberg y los Pentagon Papers", *Revista Crítica de Ciencias Sociales y Jurídicas, UCM*, nº 31, Marzo 2011, p. 11.

159 McNamara encarga la realización del estudio porque, en 1967, no se vislumbraba un final rápido para la Guerra de Vietnam.

160 El 13 de junio de 1971, *The New York Times* publicó la primera serie de archivos que había recibido de Ellsberg bajo el titular: "Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement". En la serie se revelaba cómo Ellsberg había comenzado el 1 de octubre de 1969 a hacer copias de los documentos, para demostrar que la participación de Estados Unidos en la Guerra de Vietnam se basaba en dos décadas de mentiras y de crímenes de guerra. Todo ello protagonizado por los ataques aéreos contra Laos y los bombardeos costeros en la región, antes de que incluso el Presidente Lyndon B. Johnson, sucesor de Kennedy, informara del conflicto al país en 1964.
Véase BIGELOW, Bill, & MCGAULEY, Sylvia, & MCKENNA, Tom, & HYUNG, Nam, & TREICK, Julie: *The Most Dangerous Man in America: Daniel Ellsberg and the Pentagon Papers*, Teaching guide, Zinn Education Project, Washington DC, 2010, p. 5.

161 Parafraseando al entonces consejero de Seguridad Nacional, Henry Kissinger.

162 Sánchez Hernández: "Analogías de la historia I", op. cit., p. 11.

acontecimientos que habían alterado el proceso[163] decidió absolver a los acusados, convirtiendo desde aquel momento a Ellsberg en fuente de inspiración para la denuncia de la mentira y el exceso gubernamental.

Del mismo modo, aunque ya en la década de los ochenta, Ronald William Pelton, especialista en comunicación en la *NSA*, para la que trabajó durante 14 años, fue identificado por un desertor soviético,[164]como enlace de información del *KGB* con la estructura de inteligencia interna de la *NSA*. Muy similar al caso protagonizado por Walker, Pelton, igualmente acuciado por deudas personales comenzó una aproximación a los servicios de inteligencia soviéticos a partir de enero de 1980.[165]El 20 de diciembre de 1985 fue acusado de seis cargos relacionados con el espionaje. Tras un juicio muy publicitado fue condenado el 5 de junio de 1986, por conspiración y dos cargos de espionaje.[166]

Por su parte, en 1988 Margaret Newsham fue la responsable de la primera divulgación pública sobre el sistema de vigilancia *ECHELON*.[167]Empleada en la *NSA*, entre 1974 y 1984 desarrolló su trabajo para contratistas como *Ford* o *Lockheed Martin*,[168]hasta que en 1988 desveló cómo la Agencia era capaz desde finales de la década de los 70 de rastrear a una persona determinada y captar su conversación telefónica en tiempo real, gracias a programas de software que eran conocidos con los nombres en clave *SILKWORTH* y *SIRE*,[169]mientras que *ECHELON* era el nombre de la red de vigilancia.

La controversia sobre *ECHELON* abarcó toda la década de los 90 hasta que en el año 2001 el Parlamento Europeo inició una investigación que acabaría demostrando la existencia de este programa, que operaba bajo la "*cooperación proporcionada entre los Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda, es decir, en el marco del Acuerdo UKUSA, para interceptar comunicaciones privadas y comerciales, así como las comunicaciones no militares*".[170]El programa fue revelado en 1988 en la revista británica *The New Statesman*[171] por el periodista de investigación Duncan Campbell,[172]quien también fue el encargado de elaborar en 1999 el informe *Interception Capabilities 2000* para el Parlamento Europeo,[173]donde se desgrana el funcionamiento de *ECHELON* y su impacto sobre *COMINT*. No obstante, ya en 1996 el responsable de describir los detalles sobre el funcionamiento de la red fue el también periodista Nicky Hager, a través de su libro "*Secret Power*".[174]Por medio de una serie

163 Como el intento de robo en la oficina del psiquiatra de Ellsberg o las reuniones entre el juez Byrne y un alto asesor de Nixon, John Ehrlichman, donde se le ofreció al juez la dirección del FBI.
Véase Bigelow, McGauley, McKenna, Hyung, Treick O'Neill: *The Most Dangerous Man in America*, op. cit., p. 59.
164 En julio de 1985, el coronel de la *KGB* que tuvo contacto inicial con Pelton en Washington D.C, Vitaly Yurchenko, desertó a los EEUU y proporcionó información que condujo a su procesamiento.
165 Declaró la quiebra con unas deudas de más de 65.000 dólares. Supuestamente recibió 35.000 dólares de los soviéticos entre 1980 y 1983 a cambio de facilitar información sobre los programas de recolección de inteligencia de Estados Unidos.
166 El 6 de diciembre de 1986, Pelton fue sentenciado a cumplir tres cadenas perpetuas.
167 Creado a finales de los sesenta con el objetivo de supervisar las comunicaciones militares y diplomáticas de la URSS y sus aliados del bloque del este en el contexto de la Guerra Fría.
168 Es una multinacional de origen estadounidense dedicada a la industria aeroespacial y militar. Se trata del mayor contratista militar del país.

169 European Parliament: *Report on the existence of a global system for the interception of private and commercial communications* (*ECHELON* interception system), 11 July 2001, p. 71 en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001- 0264+0+DOC+PDF+V0//EN
170 Ibíd., op. cit., p. 133
171 CAMPBELL, Duncan: "They've got it taped", August 12, 1988, *The New Statesman*, en: http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman- 1988/They've%20got%20it%20taped.pdf
172 Especializado en servicios de inteligencia, seguridad y defensa y libertades civiles.
173 CAMPBELL, Duncan: *Interception Capabilities 2000*, Edinburgh, April 1999, en: http://fas.org/irp/eprint/ic2000/ic2000.htm
174 HAGER, Nicky: *Secret Power*: *New Zealand's Role in the International Spy Network*, Ed: Potton &Burton, September 1996.

de entrevistas con más de 50 personas que fueron empleados por el servicio de inteligencia neozelandés, el *GCSB*,[175]y que participaron en las actividades del programa, Hager, dio a conocer al mundo el sistema de interceptación global conocido como *ECHELON*.

También desde la perspectiva periodística es relevante destacar a James Bamford. Especializado en las Agencias de inteligencia estadounidenses, en concreto la *NSA*, durante la Guerra de Vietnam pasó tres años en la Marina como analista asignado a una unidad de la *NSA* en Hawái.[176]Se trata de uno de los periodistas que más ha escrito sobre la *NSA* y sobre su estructura de vigilancia.[177]Por ejemplo, según Bamford, el principal problema de Europa no es la cuestión de si *ECHELON* ha robado secretos empresariales estratégicos, sino más bien si se ha producido la violación del derecho fundamental a la intimidad.[178]

Tras el ataque terrorista del 11 de septiembre, el número de filtradores de documentos secretos se multiplicó. Uno de estos casos lo protagonizó Coleen Rowley[179] y cabe encuadrarlo en la amplia lista de denunciantes de inteligencia que evidenciaron fallos en el proceso de trabajo interdepartamental y por los que, en parte, el ataque del 11 de septiembre de 2001 acabó fraguándose con éxito.

En mayo de 2002, Rowley testificó ante el Comité Judicial del Senado sobre los acontecimientos que derivaron en el ataque terrorista del 11-S.[180]A la vez que ejercía su derecho a declarar, Rowley hizo pública una carta dirigida al Director del *FBI*, Robert Mueller, donde justificaba su declaración. En ella, Rowley pone el punto de mira en Zacarias Moussaoui, quien luego fuera arrestado por participar activamente en la serie de atentados.[181]A pesar de solicitar de forma cautelar una custodia[182] que fue denegada, tampoco el personal cualificado del *FBI* difundió las sospechas[183] a otras autoridades internas de la Agencia, lo que facilitó la dispersión y el olvido.

Pocos días después del ataque, Mueller, bajo su condición de Director, realizó unas declaraciones en las que reconocía que tal vez el *FBI* era la única oficina con información suficiente como para haber previsto el incidente y actuar en consecuencia, algo que Rowley, previendo la crítica pública a la ineficiencia de la Agencia y para que la información no se volviera en su contra, se adelantó constatando su rechazo, no hacia el personal que hizo bien su trabajo, sino hacia los estamentos elevados, a los que dirigió una férrea crítica y llegó a preguntarse acerca de si dentro del *FBI* el ataque contó con cómplices[184] que hicieron perder la línea de interés en la investigación.[185]

Con el comienzo del nuevo siglo continuarían los casos de filtraciones de actividades de la inteligencia norteamericana. Uno de los más destacados fue el protagonizado por Ray McGovern, analista de la *CIA* durante 27 años, en el período comprendido

175 *Government Communications Security Bureau*.
176 BAMFORD, James: "The NSA and Me", October 2, 2014, *The Intercept*, en: https://theintercept.com/2014/10/02/the-nsa-and-me/
177 European Parliament: *Report on the existence of a global system*, op. cit., p. 70.
178 Ibíd.
179 Ya en el año 1990 Rowley asumió el cargo de Jefe de la División de Asesoría del *FBI* en Minneapolis.
180 En su declaración, dejaba constancia de los problemas endémicos que enfrenta el *FBI* y la comunidad de inteligencia a la hora de atender todas las informaciones, con el mismo orden de relevancia.
181 Según la carta de Rowley, antes del 11-S, los agentes de la división de Minneapolis respondieron a una llamada de un informador que confirmaba el entrenamiento de vuelo de Moussaoui en un simulador *Boeing 747*, quien pasó desde aquél instante a ser identificado por la división como amenaza terrorista.
182 ROWLEY, Coleen: "Coleen Rowley's Memo to FBI Director Robert Mueller An edited version of the agent's", Washington D.C., May 21, 2002, *TIME Online Edition*, p. 1.
183 Ibíd., op. cit., p. 4.
184 En la crítica llega a citar al ex agente del *FBI*, Robert Hansen, acusado de espionaje en favor de Rusia al vender software secreto que terminó en manos del terrorista más buscado en ese momento, Osama Bin Laden.
Véase Rowley: "Coleen Rowley's Memo", op. cit., p. 9.
185 Tras asumir el error, Mueller creó una nueva oficina de inteligencia en el *FBI* centrada en contraterrorismo.

entre 1963 y 1990, desde la Administración Kennedy hasta la de George H. W. Bush. Entre sus tareas se encontraban la preparación del informe diario del Presidente que informaba a cada uno de los cinco asesores de seguridad nacional de más elevado rango durante la primera Administración de Ronald Reagan, desde 1981 hasta 1985.

Su oposición a la comunidad de inteligencia comenzó en 2003 como proceso de su retiro de las tareas de inteligencia, cuando decidió cofundar la sociedad *Veteran Intelligence Professionals for Sanity*, con el único objetivo de implicar a los veteranos retirados preocupados por los diversos problemas que azotaban a la comunidad de inteligencia.[186]

Más allá del rechazo patente al conflicto de Iraq,[187]el caso de oposición más conocido de McGovern es el de Wen Ho Lee, un científico nuclear que trabajaba para la Universidad de California en el laboratorio nacional *Los Álamos*, dependiente del Departamento de Energía, quien fue acusado de espionaje[188] y aportación de datos sobre el arsenal nuclear estadounidense a la República Popular de China en diciembre de 1999.[189]

En este primer lustro del siglo XXI se pueden observar múltiples casos de filtradores que trabajaron en la *NSA*. Uno de ellos fue Russ Tice, ex analista de la *Defense Intelligence Agency* (*DIA*)[190]y de la propia *NSA*, quien cooperó en diciembre de 2005 con *The New York Times* para dar a conocer las escuchas ilegales e inconstitucionales de ambas Agencias a dispositivos móviles de ciudadanos norteamericanos. Del mismo modo, Thomas Tamm, quien ejerciera de abogado para el *Office of Intelligence Policy and Review,*[191]también se convirtió desde 2006 en filtrador al mismo diario del incremento de las actividades de vigilancia de la *NSA*.[192]Otro caso, aunque un tanto particular fue el de Mark Klein, ex técnico de *AT&T* que dio a conocer al mundo en 2006 la cooperación entre la empresa y la *NSA* mediante la instalación de la conocida como "*Sala 641A*" para monitorizar, capturar y procesar las telecomunicaciones estadounidenses.[193]

El 13 de junio de 2007, Thomas Drake, un ex alto cargo de la *NSA* fue acusado de ser enemigo del Estado en un proceso que según señala Jane Mayer, periodista de *The New Yorker*, recordaba al empleado por el Gobierno frente a Aldrich Ames.[194]Este

186 Ya en febrero de 2003, *Veteran Intelligence Professionals for Sanity* manifestó su desacuerdo con el discurso del entonces Secretario de Estado, Colin Powell, al señalar el engaño que éste había cometido al justificar ante el Consejo de Seguridad de la *ONU* la guerra en Iraq. El rechazo al conflicto de Iraq hizo que el grupo se ganara la enemistad gubernamental hasta el punto de que para silenciarlo, de la mano de Peter Hoekstra, el Presidente del Comité de Inteligencia, se autorizó la promulgación de la Ley HR5020, por medio de la cual se llegó a contemplar la posibilidad de despojar a los veteranos de inteligencia de sus pensiones del Gobierno, algo que finalmente quedó en amenaza pues el Congreso rechazó el trámite.
Véase *Biography Ray McGovern*, en: http://www.raymcgovern.com/bio.html

187 Incluyendo una confrontación televisiva en Atlanta en 2006 con el Secretario de Defensa, Donald Rumsfeld, coincidiendo con el cambio de estrategia en Iraq durante la segunda Administración de Bush.

188 En agosto de 1999, Robert Vrooman, el ex Jefe de contrainteligencia en *Los Alamos*, confesó al *The New York Times* que la raza fue un factor clave en la decisión de investigar a Lee.

189 A pesar de que en ningún momento las acusaciones de la Fiscal del Gobierno se sustentaban estuvo nueve meses en prisión. Multitud de voces se levantaron contra el Gobierno por su actitud y McGovern manifestó en numerosas ocasiones su rechazo al Gobierno de George Bush aun cuando Lee quedó en libertad, nueve meses después.

190 La *DIA*, fue diseñada con el propósito de facilitar la coordinación y la capacidad de análisis de los servicios de inteligencia de las Fuerzas Armadas. Su misión consiste en producir y coordinar inteligencia militar para el Secretario de Estado y la Junta de Jefes de Estado Mayor.

191 Una Agencia dependiente del *United States Department of Justice* (*DOJ*).

192 BraveNew Foundation: *War on whistleblowers*. Free press and the National Security State, discussion and resource guide, p. 6, en: http://www.filmsprout.org/discussion- guides/WarOnWhistleblowersDiscussionGuide.pdf?iframe=true&width=500&height=650

193 Electronic Frontier Foundation: *Declaration of Mark Klein, unredacted, from the* case *Hepting* v. *AT&T*, June 8, 2006, p. 3, en: https://www.eff.org/files/filenode/att/ser_klein_decl.pdf

194 Oficial de la *CIA* que en las décadas de los ochenta y noventa vendía documentos de la inteligencia norteamericana al *KGB* para facilitar al Kremlin el asesinato de espías norteamericanos encubiertos.
Véase MAYER, Jane: "The Secret Sharer", May 23, 2011, *The New Yorker*, en: http://www.newyorker.com/maga-

proceso no era otro que imponer la Ley de Espionaje de 1917, que prohíbe cualquier intento de interferencia, por mínima que sea, con la intención de apoyar a enemigos de los Estados Unidos, estatuto que también se empleó para tratar de silenciar a Daniel Ellsberg tras la filtración de los *Pentagon Papers*.

Entre las acusaciones, la extracción de documentos de la sede de la Agencia en Fort Meade, Maryland, con el propósito de filtrarlos a la prensa[195] e informar así acerca de las dudosas prácticas jurídicas puestas en marcha por la Agencia bajo la coartada de su campaña contra el terrorismo.[196]En su defensa, Drake aludió a Michael Hayden, Director de la *CIA* entre 2006 y 2009, quien también ostentó el cargo de Director de la *NSA* entre 1999 y 2005, que perseguía silenciarle por su oposición al proyecto emergido tras el ataque del 11-S y conocido como *TRAILBLAZER*.[197]El programa en cuestión, dependiente de la *NSA*, consistía en un sistema avanzado de análisis de datos mediante rastreo de comunicaciones como Internet, además de contemplar facetas de seguimiento por medio de filtrado de correos electrónicos y localización telefónica.[198]

Finalmente, tal vez el caso más actual sea el de Bradley Manning. Un ex analista de inteligencia y soldado del ejército de Estados Unidos acusado por el Pentágono y condenado por un tribunal militar en agosto de 2013 a 35 años de prisión, por ser considerado el responsable de filtrar miles de cables clasificados a *WikiLeaks*.[199]Entre los cargos que en un principio se le imputaron, destacan la violación del *Uniform Code of Military Justice (UCMJ)* en dos de sus artículos, el 92[200] y el 134.[201]

El volumen de los cables secretos revelados, tal como indica Michelle Van Cleave, ha tenido repercusión en todo el mundo socavando la credibilidad de Estados Unidos o poniendo en peligro las vidas de soldados estadounidenses e informantes afganos. Van Cleave señala la falta de confianza que las revelaciones han generado, al preguntarse "*¿Quién va a*

zine/2011/05/23/the-secret-sharer

195 La acusación se fundamentó en las sospechas sobre unos artículos publicados en el diario *The Baltimore Sun*, por el periodista Siobhan Gorman. Estos artículos desvelaron información confidencial sobre prácticas jurídicas, disfunciones burocráticas y programas de lucha contra el terrorismo de la *NSA*.

196 Mayer insiste en que a pesar de que Obama cuando asumió la presidencia en enero de 2009 defendió la transparencia gubernamental, la nueva Administración estaba actuando de modo similar a la anterior con los casos de filtradores de información clasificada que se les iban presentando.

197 *TRAILBLAZER tenía las siguientes responsabilidades:*
Asegurar la transformación del Sistema Criptológico de Estados Unidos en relación a la explotación de la red global, y
Actuar como catalizador en las relaciones con el cliente y las prácticas operacionales. Comenzar la reorganización de la NSA para proveer servicios y capacidades que respondan al cambio tecnológico y las necesidades de los clientes.
Véase Office of the Inspector General of the Department of Defense: *Requirements for the TRAILBLAZER and THIN-THREAD Systems*, Deputy Inspector General for Intelligence, Audit Report, December 15, 2004, p. 28, en: http://fas.org/irp/agency/dod/ig-thinthread.pdf

198 A pesar de que el proyecto fue abandonado en 2006, se constituyó tempranamente como un fracaso de 1,2 mil millones de dólares y se utilizó como plataforma de enriquecimiento para cargos de responsabilidad de las Agencias.

199 Entre las filtraciones, el suceso conocido como "Collateral Murder" o los diarios de la Guerra de Afganistán e Iraq, además de alrededor de 150.000 cables con múltiples informaciones vinculadas a embajadas diplomáticas norteamericanas.

200 *Queda sujeta a este capítulo cualquier persona que:*
viole o no obedezca cualquier reglamento u orden general legal;
teniendo conocimiento de la orden legal emitida por un miembro superior de las Fuerzas Armadas, que sea su deber obedecer, no obedezca la orden; o
abandone el ejercicio de sus funciones, y será castigado mediante designio de la corte marcial.
Véase United States Code (*USC*) Title 10: Armed Forces, §§ 801–946: *The Uniform Code of Military Justice (UCMJ)*, Article 92: "Failure to obey order or regulation", May 31, 1951, en: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partII-chap47.pdf

201 *Todas las negligencias en perjuicio del buen orden y la disciplina en las Fuerzas Armadas, toda conducta de naturaleza tal que desacredite a las Fuerzas Armadas, y los delitos y faltas no capitales, se pondrán en conocimiento de una corte marcial general que dictaminará el castigo correspondiente según la naturaleza y gravedad del delito y será castigado según su criterio.*
Véase United States Code (*USC*), *The Uniform Code of Military Justice* (*UCMJ*), Article 134: "General Article".

*estar dispuesto a hablar con Estados Unidos ahora, viendo todos los secretos a la intemperie y el dedo apuntando potencialmente a ellos como la fuente?"*[202]

Por su parte, la *American Civil Liberties Union* (*ACLU*) mostró su pesar en un comunicado del 21 de agosto de 2013, tras conocerse la sentencia y poniendo especial énfasis en la tristeza y el error que supone que un sistema legal confunda entre lo que es filtración y lo que se debe entender por traición a la nación.[203]

## 4.2. WikiLeaks. La ventana a las revelaciones masivas.

"*En la actualidad existen setenta y cuatro millones de referencias a WikiLeaks en Google. Se dice que, en apenas tres años, el sitio ha publicado más primicias que The Washington Post en treinta*".[204]

*WikiLeaks* se ha erigido, desde el comienzo del nuevo siglo, en el estandarte de las filtraciones en lo que respecta al contingente de operaciones implementadas por el Gobierno norteamericano en respuesta a los ataques del 11 de septiembre de 2001. Como su propia página web indica, el proyecto *WikiLeaks* centra su principal interés en los regímenes totalitarios, como China, la Eurasia Central, el Próximo Oriente y África Subsahariana; lo que no impide cooperar abiertamente con aquéllas fuentes o agentes que denuncien revelaciones que pongan en tela de juicio el comportamiento ético de sus respectivos Gobiernos incluyendo las democracias más asentadas y persiguiendo el objetivo de remover conciencias jugando para ello con la baza de la información.[205]Hasta el presente año, *WikiLeaks* ha recibido más de 1,2 millones de documentos.

Desde su comienzo en 2001, el enfoque geopolítico-totalitario de *WikiLeaks* orientado hacia los regímenes represivos de Eurasia y Oriente Medio, sin duda, apelaba a lo que Estulin identifica como un "*doble discurso Orwelliano*".[206]Incluso la metodología de revelación de secretos de Gobiernos extranjeros estaba acorde con las prácticas propias de las operaciones encubiertas estadounidenses, dirigidas a provocar desde cambios de régimen a impulsar revoluciones de colores.

La duda acerca de su composición original fue despejada a comienzos de 2007 cuando la propia organización reconoció que el proyecto se había levantado gracias a las aportaciones de "*disidentes chinos, matemáticos y tecnólogos de compañías startup de Estados unidos, Taiwán, Europa, Australia y Sudáfrica, representantes de comunidades de refugiados expatriados de Rusia y el Tíbet, periodistas, un antiguo analista de la inteligencia estadounidense y criptógrafos*".[207]No obstante, como indica Estulin, el secreto mejor guardado de *WikiLeaks* continúa siendo su fuente de financiación. "*Lo que se sabe es que, según Assange, el eje de su red financiera es la Fundación Wau Holland, en Alemania*".[208]

202 VAN CLEAVE, Michelle: *Myth, Paradox and the obligations of leadership: Edward Snowden, Bradley Manning and the Next Leak*, Center for Security Policy, Occasional Paper Series, Washington DC, September 13, 2013, p. 3.
203 En el comunicado de la *ACLU* se cuestiona el doble rasero a la hora de juzgar a un soldado que comparte información con la prensa y el público y cuyo castigo es mucho más severo que otros que han torturado a prisioneros y civiles. Al mismo tiempo incide en el resultado injusto que provoca de cara al público, el privarle de información crítica necesaria para la rendición de cuentas en un sistema democrático cuando el propio sistema no distingue entre las filtraciones a la prensa por el interés público y la traición a la nación.
Véase American Civil Liberties Union (*ACLU*): *ACLU comment on Bradley Manning sentence*, August 21, 2013, en: https://www.aclu.org/news/aclu-comment-bradley-manning-sentence
204 ESTULIN, Daniel: *Desmontando WikiLeaks*, Ed: Bronce, 2011, p. 11.
205 WikiLeaks. *¿Qué es WikiLeaks.org?* en: https://wikileaks.org/wiki/Wikileaks/es
206 Estulin: *Desmontando*, op. cit., p. 30.
207 Ibíd., p. 19.
208 *Assange dijo que WikiLeaks recibe alrededor de la mitad de su dinero de donaciones modestas a través de su página web, mientras que la otra mitad procede de contactos personales, incluidas personas con poder económico que se aproximan a la organización dispuestas a donar desde 10.000 dólares a 60.000.* Véase WHALEN, Jeanne & CRAWFORD, David: "How WikiLeaks keeps its funding secret", August 23, 2010, *The Wall Street Journal*, en: http://www.wsj.com/articles/SB10001424052748704554104575436231926853198

La importancia de *WikiLeaks* en materia de filtraciones de operaciones de inteligencia supone un punto de inflexión que sin duda estimula a numerosas fuentes a la denuncia de sus Gobiernos, como sucederá años más tarde, con Edward Snowden y sus revelaciones sobre las prácticas de la *NSA*.

## 4.3. Filtraciones más relevantes de WikiLeaks.

*Baghdad airstrike*. [5/04/2010]

A las 10:44 horas del 5 de abril de 2010, *WikiLeaks* hacía público un vídeo correspondiente a información militar clasificada en el que se observa el asesinato de más de una docena de personas en el suburbio iraquí de Nueva Baghdad, contando entre ellos a Namir Noor-Eldeen y su ayudante, dos empleados de la Agencia *Reuters*, que se encontraban en el terreno realizando labores periodísticas.[209]Como indica *WikiLeaks* en su web, Reuters había estado intentando acceder a la grabación apelando a la Ley de libertad de información desde el momento del ataque.

En la grabación, tomada por el propio helicóptero apache que sobrevuela la zona, se recogen los testimonios de los militares que ejecutan el tiroteo que causa el asesinato del grupo de civiles, a pesar de que en ningún momento, existe la presencia clara de un arma[210] en el escenario. Después de continuar el tiroteo a las personas que intentan recuperar los cuerpos, los militares caen en la cuenta de que entre los caídos se encuentra una niña que necesita evacuación inmediata, algo que en la grabación recibe una cortante respuesta: "*Esto es lo que pasa por traer a sus hijos a la guerra*".[211]

Tras la investigación posterior al incidente, el ejército de Estados Unidos concluyó que los soldados habían actuado de acuerdo a las reglas de compromiso en caso de guerra, algo que *WikiLeaks* negó, entendiendo que en el artículo [212]al que aludía el ejército no existía legalidad ni amparo algunos para que un reportero fuera considerado una amenaza hostil.

*Guerra de Afganistán*. [25/07/2010]

---

209 WikiLeaks. *Collateral Murder,* 5 Apr 2010, en: https://wikileaks.org/wiki/Collateral_Murder,_5_Apr_2010

210 01:18 *I don't know if that's a...*
01:19 *Hey Bushmaster element [ground forces control], copy on the one-six.*
01:21 *Thats a weapon.*
01:22 *Yeah.*
01:23 *Hotel Two-Six; Crazy Horse One-Eight [second Apache helicopter].*
01:29 *Copy on the one-six, Bushmaster Six-Romeo. Roger.*
01:32 *Fucking prick.*
01:33 *Hotel Two-Six this is Crazy Horse One-Eight [communication between chopper 1 and chopper 2]. Have individuals with weapons.*
01:41 *Yup. He's got a weapon too.*
01:43 *Hotel Two-Six; Crazy Horse One-Eight. Have five to six individuals with AK47s [automatic rifles]. Request permission to engage [shoot].*
01:51 *Roger that. Uh, we have no personnel east of our position. So, uh, you are free to engage. Over.*
02:00 *All right, we'll be engaging.*
02:02 *Roger, go ahead.*
02:03 *I'm gonna... I can`t get 'em now because they're behind that building.*
02:09 *Um, hey Bushmaster element...*
02:10 *He's got an RPG [Rocket Propelled Grenade]?*
02:11 *All right, we got a guy with an RPG.*
02:13 *I'm gonna fire.*
02:14 *Okay.*
WikiLeaks: *Baghdad Airstrike/Collateral Murder*, April 5, 2010, 01:18-02:14, en: https://www.youtube.com/watch?v=Ojw5MnsqkJQ

211 17:04 *Roger, we need, we need a uh to evac [evacuate] this child. Ah, she's got a uh, she's got a wound to the belly.*
17:10 *I can't do anything here. She needs to get evaced. Over.*
17:18 *Bushmaster Seven, Bushmaster Seven; this is Bushmaster Six Romeo.*
17:20 *We need your location over.*
17:25 *Roger, we're at the location where Crazyhorse engaged the RPG fire break.*
17:37 *Grid five-four-five-eight.*
17:46 *Well it's their fault for bringing their kids into a battle".*
Ibíd., 17:04-17:46.

212 *Las Fuerzas de los Estados Unidos siempre pueden utilizar la fuerza, incluyendo la fuerza letal, para neutralizar y/o detener a las personas que cometan actos hostiles o exhiban intención hostil contra las Fuerzas estadounidenses o de la coalición.*
WikiLeaks. *US Iraq Rules of Engagement leaked*, February 4, 2008, en: https://wikileaks.org/wiki/US_Iraq_Rules_of_Engagement_leaked

El 25 de julio de 2010, *WikiLeaks* hacía públicos los casi 77.000 registros acaecidos durante la guerra de Afganistán entre enero de 2004 y diciembre de 2009.

El conocido como diario de la guerra de Afganistán[213] detalla cada una de las acciones militares letales o no letales que implican a militares estadounidenses. Además de revelar la ubicación geográfica precisa y los acontecimientos u operaciones detrás de las muertes, se encarga de especificar el número de personas expuestas,[214]convirtiéndose en el archivo de guerra más importante sobre la realidad de un conflicto, toda vez que en el momento de su difusión, las intervenciones seguían produciéndose. Del mismo modo, la información resulta del todo completa, dado que también figuran las acciones propias de la rutina diaria, como hablar con los ancianos de la aldea, el compromiso con fuerzas hostiles, los secuestros o las operaciones de inteligencia para interceptar las comunicaciones de radio enemigas e incluso de la policía afgana.

Tal como se encarga de detallar *WikiLeaks*, este archivo muestra "*la gran variedad de pequeñas tragedias que casi nunca son informadas por la prensa, pero que representan la gran mayoría de las muertes y lesiones en el conflicto*".

*Guerra de Irak*. [22/10/2010]

El 22 de octubre de 2010, *WikiLeaks* publicó la filtración de información clasificada militar más importante de la historia: 391.832 informes que documentaban los sucesos de la guerra de Irak desde el 1 de enero de 2004 al 31 de diciembre de 2009 (excepto los meses de mayo de 2004 y marzo de 2009).[215]En los informes se detallan hasta 109.032 muertes,[216]de las cuales 66.081 corresponden a civiles y 23.984 al catalogado como grupo insurgente. *WikiLeaks* constata que los informes son el resultado de "*lo visto y oído por las tropas militares estadounidenses sobre el terreno de Irak y son la primera visión real de la historia secreta de la guerra de la que el Gobierno de Estados Unidos ha estado al tanto en todo momento*".[217]

Departamento de Estado. *Cablegate*. [28/11/2010]

El 28 de noviembre de 2010, *WikiLeaks* hacía públicos un total de 251.287 cables de información confidencial de las diferentes embajadas norteamericanas. Los cables, que contienen información desde 1966 hasta febrero de 2010, revelan documentos públicos concernientes al total de 274 embajadas, consulados y misiones diplomáticas en países de todo el mundo. Un global de 261.276.536 palabras, siete veces más que el tamaño de los documentos relativos a la guerra de Irak.

Como *WikiLeaks* señala, en estos documentos se recogen desde la iniciativa de espionaje a los aliados como el cabildeo de las corporaciones estadounidenses sobre el terreno de los países anfitriones.

*Global Intelligence Files leak*. [27/02/2012]

El 27 de febrero de 2012, *WikiLeaks* publicó más de cinco millones de correos electrónicos de la empresa de inteligencia global, con sede en Texas: *Stratfor*. Los correos datan del período comprendido entre julio de 2004 y finales de diciembre de 2011. Los correos demuestran que la compañía ofrece sus servicios de inteligencia confidencial

213 WikiLeaks. *Afghanistan war logs*, July 25, 2010, en: https://wikileaks.org/afg/
214 Incluyendo el número de personas fallecidas, heridas o detenidas en el transcurso de cada acción, junto con la ubicación geográfica precisa de cada caso y las unidades militares involucradas así como el armamento empleado.
215 WikiLeaks. *Iraq War Logs*, October 22, 2010, en: https://wikileaks.org/irq/
216 *La mayoría de las muertes (66.000, más del 60%) corresponden a civiles. Esto significa que, cada día han muerto 31 civiles, durante un período comprendido de 6 años de conflicto. Si se compara con el diario de la guerra de Afganistán, en el mismo período se registraron aproximadamente unas 20.000 muertes de civiles*.
Ibíd.
217 Ibíd.

a grandes corporaciones [218]dependientes del Gobierno norteamericano, entre ellas, el propio el *US Department of Homeland Security* (Departamento de Seguridad Nacional). De la misma forma, los correos revelan la estructura propia de *Stratfor* y el cúmulo de informantes[219] que operan desde dentro de los Gobiernos internacionales y que ponen a disposición de sus clientes.

## 4.4. Edward Snowden. ¿Héroe o traidor?

"*La verdadera medida del valor de una persona no es aquello en que dice que cree, sino en lo que hace para defender esas creencias [...] No quiero ser una persona que tiene miedo de actuar en defensa de sus principios*".[220]

Corría el día 6 de junio de 2013 cuando el ex analista de la *NSA*, Edward Snowden, por fin veía cara a cara a Glenn Greenwald, el informador del diario *The Guardian,* a quien había decidido confiar las revelaciones que estarían a punto de hacer tambalear los cimientos de la comunidad de inteligencia norteamericana. El escenario, el Hotel Mira de Hong Kong, adonde Snowden había puesto rumbo sin ocultar su rastro, pues en sus propias palabras, "*no puedes iniciar una oposición contra las Agencias de inteligencia más poderosas del mundo y estar libre de riesgos. Si quieren alcanzarte, lo harán en su momento*".[221]No obstante, la filtración al periodista de *The Guardian* en junio de 2013, no fue sino la cima de un proceso iniciado en el año 2009.

Edward Snowden nace en Carolina del Norte y crece en Maryland. Hijo de empleados del Gobierno federal de clase media baja, en 2004, a los 20 años, ya se había alistado en el ejército para luchar en la guerra de Iraq. Tras regresar del conflicto[222] y a pesar de haber abandonado la secundaria, sus capacidades avanzadas para la tecnología le hicieron merecedor de un puesto como experto técnico de la *CIA* en 2005. A partir del año 2007, gracias a un anuncio de la *CIA* que suponía trabajar con sistemas informáticos en el extranjero,[223]consiguió dar el salto a filiales contratistas[224] ubicadas más allá de los Estados Unidos.

A partir de 2009,[225]Snowden comenzó a contemplar la posibilidad de delatar el conjunto de ilegalidades que estaba cometiendo la *CIA*. Así pues, regresó a Estados Unidos y, tras trabajar durante unos meses para la contratista de la *NSA*, la *Dell Corporation*, a partir de 2010 fue destinado a unas ins-

218 Proporciona servicios de inteligencia geoestratégica a grandes corporaciones como: *Bhopal's Dow Chemical Co.*, *Lockheed Martin*, *Northrop Grumman*, *Raytheon* y a Agencias gubernamentales tales como el *US Department of Homeland Security*, el *US Marines* y la *US Defense Intelligence Agency*.

219 Los archivos de la filtración han demostrado cómo Stratfor ha reclutado una red global de informantes que son pagados a través de cuentas bancarias en Suiza y tarjetas de crédito prepago. Stratfor mantiene una red de informantes tanto encubiertos como abiertos a sus clientes, lo que incluye tanto a empleados del Gobierno como a personal de embajadas y periodistas de todo el mundo. Véase WikiLeaks. *Global Intelligence Files leak*, February 27, 2012, en: https://wikileaks.org/gifiles/

220 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., pp: 62-63.

221 GREENWALD, Glenn: *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things*, Interview Hotel Mira Hong Kong, June 6, 2013, *The Guardian*, 06:04-06:19, en: https://www.youtube.com/watch?v=5yB3n9fu-rM

222 Cuando se hubo roto las dos piernas en un accidente aéreo, dejó el ejército. Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 57.

223 Tal como indica Greenwald, trabajó para la *CIA* en Suiza y estuvo destinado en Ginebra tres años, hasta 2010, bajo la tapadera de ciertas credenciales diplomáticas, pero fue a finales de 2009, al término de su estancia en Ginebra, cuando empezó a contemplar la posibilidad de filtrar secretos.

224 En la actualidad un total de 260 empresas trabajan en programas clasificados como secretos (un 13% del total de 2.000 empresas contratadas por la NSA). Entre éstas destacan gigantes de la industria de defensa estadounidense como *Booz Allen Hamilton*, *L-3 Communications*, *CSC*, *Northrop Grumman*, *General Dynamics* y *SAIC*. En el caso particular de Edward Snowden, las únicas empresas reveladas como contratistas de la *NSA* para las que trabajó, fueron *Dell Corporation* y *Booz Allen Hamilton*.

225 El propio Snowden, como recoge Greenwald, no reveló secretos en el mismo 2009 debido a la elección como Presidente de los Estados Unidos de Barack Obama. Esperaba que de algún modo, la nueva Administración acabara con los excesos en materia de espionaje de la etapa Bush.
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., pp: 59-60.

talaciones militares de la *NSA* en una base en Japón y se le concedió un nivel de acceso a secretos de vigilancia mucho mayor que el que había tenido antes, lo que le permitió realizar un volcado de información más completo que el que inició a partir de 2009.

Cuando en 2011 terminó su temporada en Japón para la *NSA*, Snowden volvió a trabajar para la *Dell Corporation*, esta vez en una oficina de la *CIA* en Maryland.[226]En 2012, es trasladado por la *Dell Corporation* de Maryland a Hawái. Así pudo pasar períodos de 2012 cargando los documentos que después serían revelados y solicitar un puesto de trabajo ofertado por la contratista *Booz Allen Hamilton* en Hawái.[227]

Aprovechando un permiso el 20 de mayo de 2013 para recibir tratamiento contra la epilepsia salió de Hawái, donde residía con su mujer y llegó a Hong Kong,[228]donde no sin tenerlo todo previsto contactó con los periodistas Glenn Greenwald y Laura Poitras.

Durante la entrevista, Snowden reconoce que la *NSA* se encuentra espiando y almacenando información de millones de ciudadanos en todo el mundo,-[229]violando sus derechos gracias a sofisticados softwares que permiten actuar de forma sigilosa y que avanzan progresivamente en sus prestaciones.[230]Tal como él mismo asegura, "*si te das cuenta de que eso es el mundo que ayudaste a crear y que va a empeorar con las próximas generaciones, extendiendo las capacidades de esta arquitectura de la opresión, estás dispuesto a aceptar cualquier riesgo con tal de que el público llegue a tomar sus propias decisiones acerca de cómo eso se aplica*".[231]

Según Greenwald, además de la negativa a dejarse llevar por el miedo, una de las motivaciones por las que el analista decidió salir a la luz y compartir tales revelaciones era la preocupación que le supuso entender que todas estas prácticas se estaban llevando a cabo a espaldas de los ciudadanos. Insistiendo en que el objetivo de Snowden no era destruir la capacidad de la *NSA* para eliminar la privacidad, admitía sin embargo, que buscaba provocar "*un debate mundial sobre la privacidad, la libertad en Internet y los peligros de la vigilancia estatal*".[232]A la vez que aclaraba que su intención no era *"destruir estos sistemas, sino ayudar a la gente a decidir si deben seguir actuando igual o no"*.[233]

Finalmente, otra motivación que Greenwald cita como clave para que Snowden actuara de la manera en que lo hizo es el excesivo poder en manos de unos pocos. Como el propio Snowden señala: "*Me sentiré satisfecho si quedan al descubierto, si quiera por un instante, la federación de la Ley secreta, la*

226 Como señala el propio Snowden: "en este puesto, veía de primera mano que el estado, sobre todo la *NSA*, trabajaba conjuntamente con la industria privada de alta tecnología para conseguir acceso total a las comunicaciones de la gente. […] Estaban creando un sistema cuya finalidad era eliminar la privacidad a escala mundial, de manera que toda comunicación electrónica pudiera ser recogida, almacenada y analizada por la *NSA*".
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 65.

227 La oportunidad era perfecta, puesto que *Booz Allen Hamilton* es una de las empresas contratistas de defensa más grandes y poderosas del país, lo que le permitiría tener acceso a datos y documentos mucho más detallados.

228 Aun siendo semiindependiente, Hong Kong forma parte del territorio chino, con lo que para los agentes americanos, una vez revelada su identidad como la fuente reveladora de las filtraciones, les sería más difícil actuar allí.

229 *La NSA y la comunidad de inteligencia están centrados en obtener la mayor cantidad posible de inteligencia, mediante cualquier método. Originalmente se observaba que estas actividades se orientaban más allá de las fronteras domésticas, pero ahora nos damos cuenta de que también somos objetivo de vigilancia. Al hacer eso, la NSA orienta sus esfuerzos a las comunicaciones de todo el mundo.*
Greenwald: *NSA whistleblower Edward Snowden*, op. cit., 02:14-02:46.

230 *Porque incluso si usted no está haciendo nada malo, estará siendo observado y registrado, además, la capacidad de almacenamiento de estos sistemas y programas aumenta cada año de forma considerable.*
Ibíd., 07:12-07:23.

231 Ibíd., 06:50-07:09.

232 Una de las hipótesis de la que parte Greenwald para justificar la motivación de Snowden en llevar a cabo las revelaciones es la necesidad de informar a los ciudadanos de EEUU y del mundo entero para que supieran qué se estaba haciendo con su privacidad, darles esa información.

233 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 64.

*indulgencia sin igual y los irresistibles poderes ejecutivos que rigen el mundo que amo*".[234]

El debate sobre la percepción de Snowden como héroe o traidor nacional también ha entrado en campaña electoral, especialmente entre los candidatos demócratas a la Casa Blanca, con vistas a la elección del nuevo Presidente en enero de 2017. La candidata Hillary Clinton considera que el ex analista de la *NSA* ha revelado información altamente confidencial que puede haber caído en las manos equivocadas comprometiendo así la seguridad nacional. Por esta razón, Clinton es partidaria de la autoridad del Gobierno[235] y de la vuelta de Snowden a suelo norteamericano para que responda por sus revelaciones. Por su parte, el otro candidato demócrata Bernie Sanders, más libertario en lo que respecta a temas de derechos civiles, confiere a Snowden la vitola de educador del pueblo norteamericano, dada su valentía a la hora de revelar prácticas ilegales del Gobierno sin miedo a represalias.

Aunque aún hoy resulta difícil dirimir si Edward Snowden es un traidor o un héroe, lo que queda claro es que se ha erigido en un nuevo punto de inflexión de la comunidad de inteligencia norteamericana. La diferencia radica en que ahora la comunidad no se ve obligada a alterar sus funciones y procesos como mecanismo de respuesta ante desafíos internacionales o confrontaciones de naturaleza bipolar, sino como respuesta a un escenario de escándalos que siembra de dudas la vigilancia nacional y su diplomacia internacional. Por esta razón, Snowden es el acontecimiento más importante que afronta la inteligencia norteamericana en este momento. Aunque la comunidad de inteligencia se ha esforzado en presentar a Edward Snowden como un traidor a la nación, no es menos cierto que la eficacia antiterrorista de los programas de vigilancia[236] no constituye suficiente prueba para demostrar que las revelaciones del ex analista pudieran comprometer al país.

## 5. Programas de espionaje masivo de la NSA revelados por Edward Snowden.

"*Cuando ellos escogen un objetivo pueden seguir sus pasos exactos. Sólo con una tarjeta de crédito y una de metro. Como, a dónde vas, qué compras y vinculando esos datos con otras personas con planes de viaje similares, pueden averiguar con quién hablan y con quién se reúnen*".[237]

### 5.1. Tratado UKUSA. Construyendo la estructura de espionaje. El club de "Los Cinco Ojos".

Para conseguir la expansión de los programas de inteligencia más allá de las fronteras norteamericanas, además de contar con el apoyo de algunas corporaciones nacionales e internacionales especializadas en el ámbito de las telecomunicaciones, la *NSA* también cuenta con el respaldo político de lo que algunos autores coinciden en nombrar "*el Club de los Cinco Ojos*". Nacido durante la II Guerra Mundial como resultado de la cooperación en materia de inteligencia, entre el Gobierno británico y los Estados Unidos, y coronado bajo la firma del acuerdo *UKUSA* de 1946, con la guerra ya finalizada. En 1948 vivió su primera ampliación con la adhesión de Canadá y en 1956, cerraba el círculo, con las incorporaciones de Australia y Nueva Zelanda. Unas adhesiones graduales que cabe entenderlas en el contexto bipolar marcado por la integración del

234 Ibíd., 47-48.
235 Al fin y al cabo no hay que olvidar su voto en favor de la *USA PATRIOT ACT* en 2001.
236 Pocos días después de las revelaciones de Snowden en junio de 2013, tanto el propio Obama como el Director de la *NSA*, el General Keith Alexander, destacaron el trabajo de los programas de la Agencia al conseguir evitar un total de 54 tramas terroristas en suelo norteamericano. No obstante, en testimonio ante el Congreso, en el mes de Octubre, ante una pregunta del Senador Patrick Leahy, Alexander retractó su primera versión y redujo el número a
13. A este hecho también hay que añadir las declaraciones del ex Vicepresidente Cheney insistiendo en que de haber dispuesto de los programas antes del 11-S el ataque se habría podido evitar, cuando en el 9/11 *Comission Report* de 2004 se dejaba constancia de la falta de operatividad entre Agencias y de las pruebas en manos del *FBI* para detectar la amenaza y evitarla, lo que habría hecho innecesario el trabajo de ningún programa de la *NSA*.
237 POITRAS, Laura, Documental: *Citizenfour*, Praxis Films, Estados Unidos, 114 min, 2014, 17:08-17:23.

bloque occidental a la *North Atlantic Treaty Organization* (*NATO)*, desde su puesta en marcha en abril de 1949.[238]

En el acuerdo original de 1946, contraído entre la *State-Army-Navy Communication Intelligence Board* (*STANCIB*) y los Departamentos de la Armada y Guerra; y el Consejo de Inteligencia de

Londres, representado por el Ministerio de Relaciones Exteriores, de la Marina, de la Guerra, el Aire y todas las demás autoridades de Comunicación de Inteligencia del Imperio Británico,[239]se enumeran las áreas de cooperación y el intercambio del tipo de productos relativos a las comunicaciones extranjeras y que van desde el criptoanálisis a las tareas de descifrado y traducción.[240]

Coincidiendo con la temprana evolución interna de la *OTAN* en la década de los cincuenta, han sido numerosos países los que se han sumado a la cooperación de inteligencia intercambiando información por medio de sus Agencias de forma autónoma. Así, países como Noruega (1952), Dinamarca (1954) o Alemania (1955) son hoy parte de este Club, aunque los lazos entre los fundadores sean mucho más profundos, de acuerdo a lo expresado por el general canadiense retirado, James S. Cox, en un escrito de diciembre de 2012, en el que explicaba el funcionamiento del grupo y su naturaleza ilimitada: "*Los vínculos que unen a los socios son desde luego mucho más profundos de lo que muchos observadores creen, pero no hay acuerdos internacionales que gobiernen todas las relaciones de inteligencia entre los Cinco Ojos*".[241]

Para Cox, las organizaciones de inteligencia de Estados Unidos, Canadá, Nueva Zelanda, Gran Bretaña y Australia, actúan de acuerdo a sus mandatos legislativos nacionales, "*con una afinidad reforzada por su cultura anglosajona común, sus aceptados valores democráticos y sus intereses nacionales complementarios, todo eso aderezado con un profundo sentido de confianza mutua y un grado de confianza profesional tan grande que es algo único en el mundo*".[242]Sin embargo, a pesar de que podría extraerse un pacto de no agresión como trasfondo en la colaboración, todos los indicios apuntan a que no hay cabida para amiguismos o afiliaciones en la esfera del Club. Se constituye así un juego basado en la cooperación pero construido sobre los cimientos de la desconfianza, donde todos sospechan de todos.

Según declaraciones ofrecidas por Edward Snowden, el Gobierno de Estados Unidos, en cooperación con estos Estados clientes del Club de los Cinco Ojos, "*ha impuesto en el mundo un sistema de vigilancia secreta y omnipresente de la que no es posible escapar*".[243]

El reparto de tal vigilancia en la geografía mundial es el siguiente, siempre de acuerdo a los términos reflejados por el ex-general Cox: "*Canadá se ocupa de zonas del norte del Atlántico y el Pacífico, parte de Rusia y China y parte de América Latina; Australia controla el sur y el este de Asia; Nueva Zelanda cubre el Pacífico sur y el sureste asiático; Reino Unido se centra en Europa y Rusia Occidental;*

238 De hecho, en este mismo contexto bipolar en 1951 se impulsa la alianza *ANZUS* (acrónimo de Australia, Nueva Zelanda y Estados Unidos) y cuyo objetivo, en el marco de la Doctrina Truman, era garantizar la seguridad en el Pacífico Sur, como medida de disuasión nuclear frente a la Unión Soviética.
239 Declassified and approved for release by NSA, Top Secret, *BRITISH-U.S. Communication Intelligence Agreement, March 5, 1946*, Declassified on April 8, 2010, en: https://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf
240 Ibíd.
241 COX, S. James: "Canada and the Five Eyes Intelligence Community", *Strategic Studies Working Group Papers*, Canadian International Council, December 2012, p. 5.
242 Ibíd.
243 Según Greenwald, protegen sus sistemas internos de la supervisión de los ciudadanos mediante clasificaciones y mentiras, y se blindan contra el escándalo de eventuales filtraciones exagerando protecciones limitadas que deciden conceder a los gobernados.
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 38.

*y Estados Unidos cubre parte de América Latina, el Caribe, China, Rusia, Oriente Próximo y África*".[244]

## 5.2. Clasificación de los objetivos de espionaje. El impulso de la cooperación y la ausencia de amistades en el entorno global.

Entre las filtraciones de Edward Snowden aparece definida la estructura de vigilancia y espionaje del ámbito internacional que protagoniza la *NSA* diferenciando su panóptico por medio de filtros entre los colaboradores principales, de los *third parties*, colaboradores no tan frecuentes, pero igual de cómplices en la vigilancia global. Tal como indica Greenwald, "*como pasa con el GCHQ, la NSA suele mantener estas relaciones pagando a los socios para que desarrollen tecnologías y se impliquen en la vigilancia, y así puede dirigir el modo de llevar a cabo la labor de espionaje*".[245]

En el documento, se observa un primer grupo responsable de la clasificación de espionaje y extensión de redes que sirvan de centinela. Estos son los países conformantes del Club de los Cinco Ojos: Estados Unidos, Australia, Canadá, Nueva Zelanda y Reino Unido, con sus correspondientes organizaciones de inteligencia. Aunque todas estas relaciones se basan en acuerdos bilaterales secretos, también hay, en el mismo peldaño, grupos selectos en los que la información de inteligencia se comparte de manera multilateral y entre los que destacan, la *NATO*, el *SIGINT Seniors Europe* (*SSEUR*), el *SIGINT Seniors Pacific* (*SSPAC*) y la *Afghanistan SIGINT Coalition* (*AFSC*).

En el siguiente peldaño, la cooperación de segundo nivel se produce con los denominados *third parties* o países del Grupo B, es decir, "*países que mantienen una colaboración limitada con la NSA y son a la vez seleccionados [por la NSA] para vigilancia agresiva no solicitada,*"[246]como señala Greenwald. Entre estos países encontramos a Alemania, la siempre estratégica Turquía, Pakistán, Corea del Sur o España, entre otros. Aunque, tal vez, la fórmula más prolífica de cooperación en este grupo aliado se produzca con Israel al mantener a veces una relación tan estrecha[247] entre la *NSA* y sus servicios de inteligencia,[248]por cuyos lazos podría casi considerarse a este aliado, como un miembro más de los Cinco Ojos.

Por último, en un peldaño inferior, ya por debajo tanto de los Cinco Ojos como de los países del mencionado Grupo B de aliados, existe una tercera categorización de extracción de inteligencia, los considerados por el Gobierno de Estados Unidos como objetivos, y nunca como socios en la elaboración de los programas de espionaje. De acuerdo a lo recogido por Greenwald, estos países son: "*Como era de esperar, Gobiernos considerados adversarios, como los de China, Rusia, Irán, Venezuela y Siria; pero también otros cuya condición oscila entre la de amigo y neutral, como Brasil, México, Argentina, Indonesia, Kenia y Sudáfrica*".[249]

Como ejemplo, se podría citar el caso de espionaje protagonizado por la *NSA*, con medios invasivos a la presidenta de Brasil, Dilma Roussef, en 2011, o al entonces candidato a la presidencia de México, Enrique Peña Nieto, así como a sus colabo-

244 Cox: "Canada and the Five Eyes", op. cit., p. 6.
245 En el documento *Foreign Partner Review* del año fiscal 2012 aparecen numerosos países que han recibido pagos de esta clase, entre ellos Canadá, Israel, Japón, Jordania, Pakistán, Taiwán y Tailandia.
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p.154.

246 Ibíd., p. 153.
247 Según Greenwald, entre los datos proporcionados a Israel se cuentan, transcripciones no evaluadas y no minimizadas, contenidos esenciales, facsímiles, télex, voz y metadatos de *DNI*. Todo ello, sin haber pasado por el proceso legalmente requerido de minimización. Estos procesos garantizan que cuando la vigilancia masiva de la *NSA* recoge datos de comunicaciones que ni siquiera las amplias directrices de la Agencia permiten reunir, esta información se destruye lo antes posible y no se difunde más. Pero si se trata de difundir datos entre la inteligencia israelí, al parecer la *NSA* ha prescindido de todas estas legalidades.
Ibíd., pp: 155-156.
248 Desde el propio *Mossad*, como responsable de las labores de inteligencia en el exterior, como el *Shin Bet*, la organización responsable de la seguridad interior, incluidos los territorios ocupados.
249 Ibíd., p. 157.

radores. El propósito de vigilar a los Gobiernos de ambos países hay que entenderlo en el marco de la influencia económica en la región de dos territorios ricos en recursos petrolíferos. De hecho, como recoge Greenwald, "*gran parte del archivo de Snowden desvelaba lo que solo cabe denominar como espionaje económico: escuchas e interceptación de emails del gigante petrolero brasileño Petrobras, de reuniones económicas en Latinoamérica, de empresas eléctricas de Venezuela y*

*México, así como espionaje efectuado por aliados de la NSA (Canadá, Noruega y Suecia) en el Ministerio de Minas y Energía de Brasil y compañías energéticas de otros países*".[250]

Aunque, tal vez, la mejor muestra del sistema de vigilancia impuesto por la *NSA* y consolidado en el juego de la desconfianza mutua son los intentos de Susan Rice, embajadora en la Organización de las Naciones Unidas (*ONU)* y asesora del Presidente Obama sobre seguridad nacional, de espiar las discusiones internas de Estados miembros de la *ONU* para averiguar sus estrategias negociadoras, especialmente en el año 2010 cuando se encontraban debatiendo sobre la necesidad, o no, de imponer nuevas sanciones al régimen iraní.[251]En el proceso, incluso países como Francia o Japón, considerados teóricos aliados, fueron espiados con el único fin de conocer su consideración previa a la votación.

250 Del mismo modo, Greenwald alude a la presencia, como objetivo de vigilancia por la *NSA*, en ese mismo archivo, del sistema bancario *SWIFT* (*Society for Worldwide Interbank Financial Telecommunication*), la petrolera Gazprom y la aerolínea Aeroflot, ambas rusas.
Ibíd., p. 167.
251 Según señala Greenwald, un documento de vigilancia similar de agosto de 2010 revela que los EEUU espiaron a ocho miembros del Consejo de Seguridad de la *ONU* en relación con una Resolución posterior sobre las sanciones a Irán. El espionaje procuró al Gobierno de EEUU valiosa información sobre intenciones de voto, lo que para Washington supuso cierta ventaja en las conversaciones con los demás miembros del Consejo de Seguridad.
Ibíd., p. 178.

Fuente: Greenwald, Snowden: Sin un lugar donde esconderse, p.154.

## 5.3. Programa PRISM.

Según Greenwald, *PRISM* es el programa más ambicioso de todos, puesto que permite a la *NSA* obtener prácticamente cualquier información de las empresas de Internet, que centenares de millones de personas de todo el mundo utilizan hoy como principal medio de comunicación. Las empresas de Internet que, según los documentos de la *NSA*, proporcionaban a la Agencia acceso directo a sus servidores como parte de *PRISM* eran: *Facebook*, *Google*, *Apple*, *YouTube* y *Skype*, entre otras.[252]

El programa posibilita a los analistas de la *NSA* la recogida de material en bruto, incluidos los historiales de búsqueda, correos electrónicos, contenido de mensajes, chats en vivo o las transferencias de archivos, de acuerdo con la publicación del diario *The Guardian* del 7 de junio de 2013,[253]momento en que el programa de vigilancia sale a la luz, gracias a las filtraciones de Edward Snowden y los periodistas Glenn Greenwald y Ewen MacAskill.

La propia cabecera plantea que, si bien las compañías han de ser conocedoras y ejercer un papel activo como cómplices del proceso; es posible que

252 Ibíd., p. 96.
253 GREENWALD, Glenn, & MACASKILL, Ewen: "NSA Prism program taps in to user data of Apple, Google and others", June 7, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

el Gobierno haya desarrollado la tecnología y la esté aplicando a espaldas[254] de estas empresas suministradoras de datos y metadatos, al manifestar algunos de sus responsables la negativa rotunda sobre la existencia de tal programa de vigilancia. En otro escenario, se confirma la total complicidad entre compañías y Gobierno, con el ejemplo de *Microsoft*, que desde el año 2007, en que comienza a operar el programa, cede los datos de sus clientes a la Agencia sin la autorización de los consumidores, convirtiéndose en el primer suministrador leal de información sujeto al programa *PRISM*. De acuerdo a una de las diapositivas del programa reveladas, el siguiente en adherirse es *Yahoo!* (el 12 de marzo de 2008), después *Google* (14 de enero de 2009) y más adelante otras corporaciones como *Facebook* (3 de junio de 2009) o *YouTube* (24 de septiembre de 2010). De la misma forma, se identifica a *Dropbox* como un futuro cooperante.[255]

Gracias a las prestaciones de este programa, la *NSA* accede mediante la organización de vigilancia más grande del mundo, a los servidores de las compañías más importantes y es capaz de almacenar la información sustraída, sin tener que obtener durante el proceso orden judicial alguna.[256]

Las reacciones no se hicieron esperar después de que *PRISM* fuera conocido por la opinión pública. Jameel Jaffer, Director del Centro para la Democracia de la *ACLU*, destacó la intromisión militar de la *NSA* en las comunicaciones civiles e insistió en que la frontera entre la Agencia y la privacidad había desaparecido.

En respuesta a las revelaciones sobre *PRISM*, El Parlamento Europeo, el 8 de junio de 2013, decidió crear la Comisión de Libertades Civiles, con la que se pretendió llevar a cabo una investigación a fondo de los programas de vigilancia de Estados Unidos. Además de obtener un respaldo masivo[257] en la propia puesta en marcha de la Comisión, los eurodiputados manifestaron su condena enérgica a las técnicas de espionaje, a la vez que pedían a Estados Unidos argumentos para defenderse de las acusaciones.

Y eso fue lo que hizo el Director Nacional de Inteligencia, James Clapper, el mismo día. Partiendo de la premisa de la falta de contexto empleada por los medios de comunicación,[258]Clapper intensificó su defensa de *PRISM,* alegando un control exhaustivo de la herramienta por parte de los tres poderes del Estado, la práctica de acciones dentro de la legalidad[259] y el derecho al silencio, por la necesidad

254 En el artículo elaborado por Greenwald y MacAskill, se recoge la postura de *Google* y al respecto de la revelación sobre el programa *PRISM* y la posible colaboración empresarial. En un comunicado *Google* dijo que varios expertos tecnológicos habían insistido en que no tenían conocimiento alguno sobre *PRISM*, literalmente argumentaron que "si lo están haciendo lo están haciendo sin nuestro conocimiento".
Ibíd.

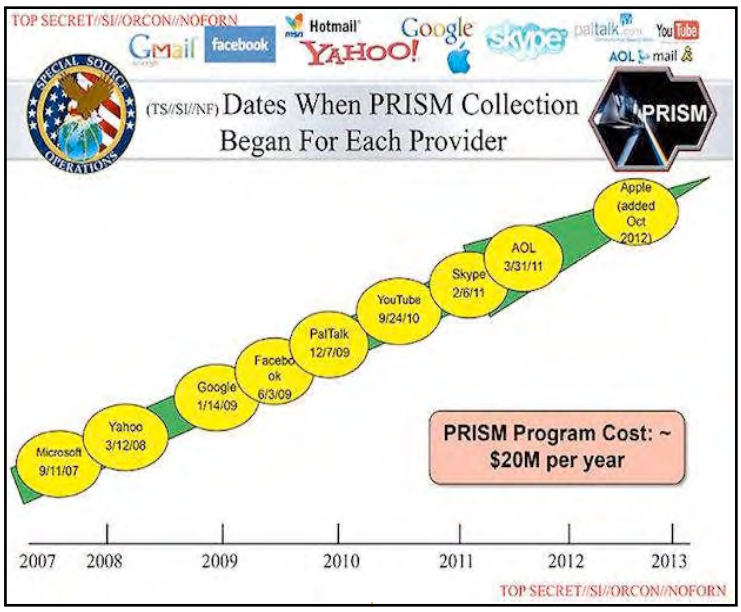
255 Un documento filtrado destaca que el número de comunicaciones obtenidas de *Skype* aumentó un 248% en 2012, un 131% en las solicitudes de datos obtenidas de *Facebook*, y el 63% en el caso de *Google*.

256 Greenwald y MacAskill señalan que el acceso de la *NSA* a los datos de las corporaciones de comunicación fue posible gracias a los cambios en la Ley de vigilancia estadounidense introducidos durante la Administración de Bush y renovados con Obama a partir de diciembre de 2012. Esa Ley permite la recolección de los datos de clientes de las empresas mencionadas que viven fuera de EEUU, pero también aquéllas personas que se comunican con otros de fuera de los EEUU o comunicaciones hechas enteramente dentro de los EEUU.
Véase Greenwald & MacAskill: "NSA Prism program taps in to user data of Apple, Google and others", op. cit.

257 La Resolución contó con la aprobación de 483 votos frente a 98 en contra y 65 abstenciones.

258 *Durante la última semana se han producido revelaciones sobre la comunidad de inteligencia que nos parecen del todo imprudentes, ya que se trata de métodos para mantener seguros a los estadounidenses. En una carrera por publicar, diferentes medios de comunicación, no han ofrecido el contexto completo, incluyendo el grado en que estos programas son absolutamente vigilados tanto por el Ejecutivo como por el Legislativo y el Judicial*. CLAPPER, R. James: *Office of the Director of National Intelligence*, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, June 8, 2013, en http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/872-dni-statement-on-the- collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act

259 *Las actividades de vigilancia publicadas estos días en The Guardian y The Washington Post, son legales y se realizan bajo el debate del Congreso y la autorización expresa del mismo.*
Ibíd.




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1979.dir/doc.pdf

de proteger las fuentes y métodos de inteligencia, en especial, de los servicios extranjeros.[260]

## 5.4. Programa BOUNDLESS INFORMANT.

El 11 de junio de 2013, *The Guardian*, de la mano de los periodistas Glenn Greenwald y Ewan MacAskill, hacía público[261] el programa *BOUNDLESS INFORMANT*, una herramienta interna de la *NSA* cuyo objetivo no se encuentra tanto en escudriñar el contenido de un email o un mensaje, sino en la relación de metadatos.[262]La filtración fue posible gracias a los documentos facilitados por Edward Snowden en las sucesivas reuniones con los periodistas del diario en el Hotel Mira de Hong Kong.

En los archivos se constata la interceptación y el almacenamiento de los datos por parte de la Agencia. Según Greenwald, dicha carpeta contenía documentos que recogían detallados datos estadísticos de la *NSA* sobre cuántos emails y llamadas interceptaba la Agencia. También contenía pruebas de que la *NSA* había estado reuniendo cada día datos de llamadas y correos electrónicos de millones de ciudadanos.[263]

*BOUNDLESS INFORMANT* no se trata sólo de un mecanismo de recolección de metadatos mediante la extracción de registros *DNI* y *DNR*,[264]sino que proporciona la capacidad a la *Global Access Operations* (*GAO*), en tanto que responsable de interceptación de señales satelitales- *SIGINT* de la *NSA*, de describir dinámicamente, sin intervención humana y mediante representación gráfica, la infor-

260 *La revelación de información sobre métodos específicos que el Gobierno emplea para recoger y almacenar las comunicaciones, obviamente, puede dar a nuestros enemigos una ventaja para saber cómo evitar la detección.*
Ibíd.

261 GREENWALD, Glenn & MACASKILL, Ewe: "Boundless Informant: the NSA's secret tool to track global surveillance data". June 11, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

262 Greenwald insiste en que, gracias a estos metadatos, queda constancia no solo de las personas con quien uno intenta comunicarse y la frecuencia, sino también de todas las personas con las que se comunican sus amigos, lo que genera un cuadro exhaustivo de la red de relaciones. Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 166.

263 Ibíd., p. 45.

264 *DNR*: (*Dialed Number Recognition*), llamadas telefónicas, y *DNI*: (*Digital Network Intelligence*), actividad en internet.
Fuente: Canadian Journalists for Free Expression/ Snowdenarchive/ https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01dc/ceab4acd.dir/doc.pdf

mación obtenida en una vista en mapas, tabla o diagramas. De la misma manera, permite a sus usuarios definir un país en la vista del mapa y ver el volumen de metadatos obtenidos, así como el histórico de recogida en el territorio.

Los documentos demuestran la capacidad de alcance del programa, poniendo de manifiesto la recolección de hasta 3 mil millones de piezas vinculadas a la inteligencia, en un período de tiempo que oscila en un intervalo de 30 días. Una de las instantáneas recogidas por la publicación, muestra un mapa de calor global, a fecha de marzo de 2013, donde se observa la capacidad de recogida y vigilancia del programa.

En ella, se observa cómo la Agencia fue capaz de recoger 97 mil millones de piezas de inteligencia de redes de ordenadores ubicados por todo el mundo, lo conocido como metadatos *DNI*, así como 124 mil millones de registros *DNR*, es decir, derivados de llamadas telefónicas. Si atendemos a los países que concentraron la mayor atención del programa, Irán destaca con la recolección de 14 mil millones de registros *DNI* y 1.7 mil millones de registros *DNR*. Le siguen, Pakistán (13.5 mil millones de *DNI* y 13.7 mil millones de *DNR*), Jordania, precisamente uno de los países árabes aliados más cercanos a Estados Unidos, (12.7 mil millones de *DNI* y 1.6 mil millones de *DNR*), Egipto (7.5 mil millones de *DNI* y 1.5 mil millones de *DNR*) e India (con 6.3 mil millones de *DNI* y 6.2 mil millones de *DNR*).

Como se puede observar, los colores también se escinden entre los sesgos de vigilancia. Así pues, los países de color verde son los menos sometidos a vigilancia, los de color amarillo, a una vigilancia intermedia y los de color naranja o rojo, donde se concentra la mayor actividad de vigilancia. Si atendemos al mapa, Estados Unidos se encuentra en el rango amarillo, lo que hace que sea susceptible de frecuentes e intermitentes interceptaciones de metadatos por el programa de la *NSA*. De hecho, en la imagen se observa una cifra sobre este territorio: 2.8 mil millones, que corresponde al número de registros *DNI* obtenidos de ciudadanos en suelo norteamericano.

La posición de la *NSA* desde agosto de 2005 y defendida por su Director, el general Keith Alexander, tal como recoge el propio *The Guardian*[265] es la de negar la existencia de tal programa por las limitaciones tecnológicas y presupuestarias existentes en la Agencia. Ante la negativa de la existencia de una vigilancia latente de los ciudadanos norteamericanos, los senadores demócratas por Oregón y Colorado, Ron Wyden y Mark Udall, también integrantes del Comité de Inteligencia del Senado, decidieron escribir el diez de octubre de 2012, una queja formal dirigida al Director de la *NSA*. En la carta muestran su disconformidad ante el hecho de que la comunidad de inteligencia siempre niegue la posibilidad de proporcionar el acceso a la estimación de comunicaciones interceptadas en virtud de las Enmiendas a la Ley *FISA* de 2008, lo que sin duda hace que sea improbable el control del Congreso y del Comité sobre las actividades de la Agencia.[266]

En una audiencia del Comité de Inteligencia del Senado celebrada en el mes de marzo de 2013, pocos meses antes de la revelación, el senador demócrata Ron Wyden se preguntaba si la *NSA* acumulaba cualquier tipo de datos de los cientos de millones de ciudadanos norteamericanos, a lo que James Clapper, Director Nacional de Inteligencia contestó

265 Preguntado acerca de si el programa tenía la capacidad para conseguir los datos, K. Alexander dijo: "No. No. No
tenemos los conocimientos técnicos ni el equipo para recoger, ni esa cantidad ni ese tipo de informaciones". Véase Greenwald & MacAskill: "Boundless Informant: the NSA's secret", op. cit.

266 Wyden y Udall, después de plantear la negativa recurrente de la comunidad de inteligencia a la hora de proporcionar la estimación acerca del número de comunicaciones interceptadas en virtud de la Ley de Enmiendas *FISA* de 2008, elaboran en su carta, sus preguntas a K. Alexander. "¿Puede indicar el número aproximado de comunicaciones de Americanos registradas?, ¿es de millones o de cientos de millones de personas? ¿Qué tan grande o pequeño sea posiblemente este número?" Véase Wyden, Ron & Udall, Mark: *Letter to General Keith Alexander*, United States Senate, Washington DC, October 10, 2012.

con un rotundo "*No, señor*".[267] *BOUNDLESS INFORMANT* parece indicar lo contrario.

## 5.5. Programa SHELLTRUMPET.

El programa *SHELLTRUMPET* comenzó el 8 de diciembre de 2007 como un analista de metadatos casi en tiempo real para un sistema de recogida clásico, tal como indica un documento filtrado[268] de la *NSA* de alto secreto en el que se reconocen las ventajas del programa, así como el salto en la recogida de datos. Según Greenwald, "*cinco años después [el programa] está procesando dos mil millones de incidentes/día y otros sistemas de la Agencia han llegado a utilizar sus capacidades de procesamiento*".[269]

El 27 de junio de 2013, el propio Greenwald y el periodista Spencer Ackerman, hacían público el programa en *The Guardian*, bajo el titular: "*How the NSA is still harvesting your online data*". En la publicación, los periodistas se hacían eco de las declaraciones de Shawn Turner, el Director para las comunicaciones de la Inteligencia nacional de la Administración Obama, donde no negaba la existencia de la herramienta aunque afirmaba su clausura en 2011: "*El programa de recolección de metadatos de Internet autorizado por el Tribunal FISA se interrumpió en 2011 por razones operativas y de recursos, y no se ha reiniciado*".[270] No obstante, en el material facilitado por Snowden se observa una cantidad ingente de metadatos de Internet almacenados por la *Special Source Operations (SSO)*,[271] desde 2011 hasta la actualidad.

Aunque el cerco de vigilancia en lo que respecta al ámbito nacional se refiere especialmente a extranjeros residentes, no está claro el volumen de recolección que el programa lleva a cabo tomando como objetivos a estos perfiles de individuos, ni el obtenido mediante la relación de metadatos, de los civiles norteamericanos. En el artículo, el diario señala cómo un funcionario de la *SSO*[272] confirma la existencia del programa, la expansión sorprendente en poco tiempo de sus capacidades de recolección y la prestación al resto de programas que supone *SHELLTRUMPET*.

## 5.6. Programa X-KEYSCORE.

Según declaraciones del propio Edward Snowden, *X-Keyscore* es el sistema interfaz que los analistas emplean para consultar, esa especie de océano de señales de inteligencia satelital en bruto obtenidas de otros programas. "*Todas esas cosas donde pueden ordenar, hacer búsquedas retroactivas, búsquedas en vivo, señalar lo que no sirve. X-Keyscore es la entrada para eso*".[273] Además, indica que desde el año 2011, la simultaneidad en la monitorización de mil millones de teléfonos móviles y sesiones de Internet se hace, gracias a esta herramienta, "*a un ritmo de 125 Gigabytes por segundo, lo que es un Terabit en diez segundos*".[274]

Greenwald, plantea la relevancia de este programa en las operatividades diarias de la Agencia, desde el prisma de un sistema de máximo alcance para reunir los datos electrónicos. "*Incluso permite un seguimiento en tiempo real de las actividades de una persona o buscar datos del sistema mediante di-*

267 Senator Ron Wyden questions Director of National Intelligence, James Clapper, *Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?*, March 2013, *The Guardian*, en: http://www.theguardian.com/world/video/2013/jun/07/privacy-wyden-clapper-nsa-video

268 Con el título: "SHELLTRUMPET Processes it's One Trillionth Metadata Record".

269 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 125.

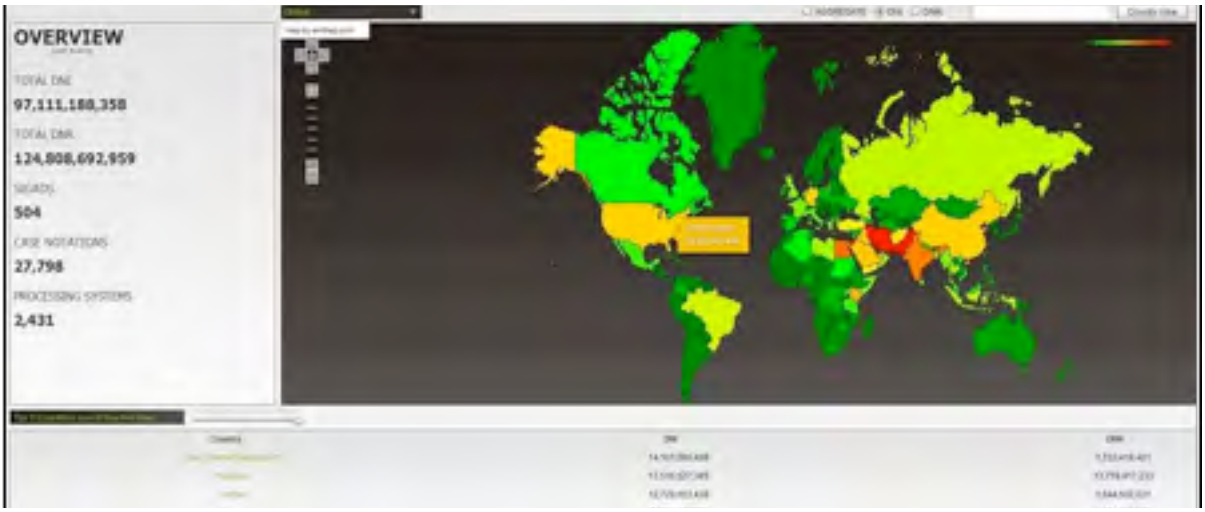
270 GREENWALD, Glenn & ACKERMAN, Spencer: "How the NSA is still harvesting your online data", June 27, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

271 En tanto que división interna de la Agencia responsable de aquellos programas y herramientas de recolección de datos tanto a nivel nacional, como más allá de las fronteras norteamericanas.

272 En su artículo, Greenwald y Ackerman recogen el testimonio del funcionario de la *SSO*. "En sus cinco años en activo, numerosos sistemas a través de la Agencia han llegado a emplear las capacidades de *SHELLTRUMPET*, sobre todo para tareas de monitorización". Véase Greenwald & Ackerman: "How the NSA is still harvesting your online data", op. cit.

273 Poitras, *Citizenfour*, 2014, op. cit., 42:20 - 43:13.

274 Ibíd. 42:20-43:13.




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01dc/ceab4acd.dir/doc.pdf

*recciones electrónicas, números de teléfono o rasgos identificadores como una IP*".[275]

En el artículo publicado por el propio Greenwald en *The Guardian* el 31 de julio de 2013, donde se informa a la opinión pública por vez primera acerca de la existencia de *X-Keyscore*, Snowden reconoce la facilidad de acceso a la privacidad de los ciudadanos mediante esta herramienta con tan sólo el conocimiento de una cuenta de email,[276]a la vez que el periodista pone de manifiesto cómo, sin ningún tipo de autorización previa, los analistas acceden a información personal[277] de millones de personas a través de una herramienta complementaria conocida como *DNI*

*Presenter*.[278]De la misma manera, una instantánea revelada identifica la presencia y expansión geográfica del programa en el mundo. Concretamente se encuentra presente en 150 países, si atendemos a que en total en el mundo hay 194 países, esto significa que *X-Keyscore* proporciona datos de inteligencia del 79,3% del territorio mundial y lo hace gracias a la interacción con las sedes centrales de la *NSA*, de los más de 700 servidores de que dispone y con los que consigue registrar, con la cooperación abierta de los servicios alemán y británico de inteligencia.

Tal como se señala en la publicación, de acuerdo a la legislación vigente estadounidense, la *NSA* requiere de una orden *FISA* individualizada, sólo si el objetivo de vigilancia fuera una persona estadounidense, sin necesitarla para interceptar las comunicaciones de estadounidenses con objetivos extranjeros. No obstante, ahí entra en juego *X-Keyscore*, proporcionando la capacidad tecnológica, "*para apuntar incluso a personas de Estados Unidos bajo la amplia vigilancia electrónica, sin orden judicial, siempre que alguna información a través de su correo electrónico o registro DNI resulte sospechosa*".[279]

275 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 189.
276 Según comenta Snowden en la entrevista realizada por Greenwald, "para buscar mensajes de correo electrónico, un analista usando X-Keyscore introduce la dirección del correo de la persona en una simple búsqueda, junto con la justificación de la misma y seleccionando el intervalo de tiempo que se desea observar".
Véase GREENWALD, Glenn: "XKeyscore: NSA tool collects nearly everything a user does on the internet", July 31, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
277 Entre esta información personal se cuentan mensajes de correo electrónico, chats en línea y los historiales de navegación por Internet.
278 Se emplea para la lectura de contenido de los correos electrónicos almacenados, así como el contenido de los chats o mensajes privados de *Facebook*, que hayan podido ser interceptados.
279 Greenwald, Glenn: "XKeyscore: NSA tool collects

## 5.7. Programa PROJECT BULLRUN.

Como indica Greenwald, *PROJECT BULLRUN* es un esfuerzo conjunto entre la *NSA* y su equivalente británico el *Government Communications Headquarters* (*GCHQ)*,[280] para derrotar las formas más habituales de encriptación en las transacciones *online*, "*hasta iniciativas a menor escala con nombres jactanciosos como: JIRAFA EGOÍSTA (permite el anonimato en la navegación), MUSCULAR (invasión de redes de Google y Yahoo!), u OLYMPIA (programa de vigilancia que ejerce Canadá sobre el Ministerio de Minas y Energía de Brasil)*".[281]

El programa salió a la luz el 6 de septiembre de 2013, cuando los periodistas James Ball, Julian Borger y Glenn Greenwald publicaron en *The Guardian* las cooperaciones en clave de inteligencia entre los servicios de Estados Unidos y Reino Unido bajo el titular: "*Revealed: how US and UK spy agencies defeat Internet privacy and security*".[282]

En el artículo se incide en que los archivos facilitados por Snowden demuestran cómo el Gobierno norteamericano ha desarrollado una tecnología capaz de desencriptar cualquier tipo de información confidencial de los usuarios en la red, desde registros médicos a banca en línea, con lo que la *NSA* habría comprometido gravemente las garantías de confidencialidad que las empresas de Internet proporcionan a sus consumidores, al asegurarles que ninguna de sus comunicaciones podrá ser perforada, ni por delincuentes ni por Gobiernos. Además de identificar que el *GCHQ* (cuyo nombre del programa homólogo es *EDGEHILL)* ha estado trabajando para desarrollar fórmulas de desencriptación en el tráfico cifrado de cuatro de los proveedores más importantes de Internet: *Hotmail*, *Google*, *Yahoo!* y *Facebook*; la publicación se hace eco de la principal defensa de las Agencias acerca de la necesidad de luchar contra la encriptación. La excusa resulta doble, por un lado la lucha contra el terrorismo, por otro, la protección de la privacidad civil frente a las amenazas en la red. Sin embargo, los expertos, como Bruce Schneier, especialista de cifrado del Centro Berkman de Harvard para Internet y Sociología, insiste en que la *NSA* y el *GCHQ* socavan la confianza de Internet y atacan la privacidad de todos los usuarios.[283]

*PROJECT BULLRUN* implica múltiples fuentes contra protocolos de uso extendido en línea como puedan ser, *HTTPS* o *Secure Sockets Layer* (*SSL*) utilizado para proteger las compras en línea. Con las herramientas que la *NSA* le proporciona, *BULLRUN* es capaz de deshacer cualquier encriptación y tener acceso pleno a la información, por muy confidencial que esta pueda llegar a ser.

La publicación también se encarga de destacar que el programa está diseñado para insertar vulnerabilidades en los sistemas de cifrado comerciales, mucho más accesibles al programa e importantes, dado el enfoque mundial de las corporaciones comerciales tecnológicas y la alta probabilidad de poder desencriptar dispositivos modernos repartidos por todo el mundo, como los que disponen de tecnología *4G*. Por su parte, las empresas tecnológicas sostienen que únicamente trabajan con las Agencias cuando están legalmente obligadas a hacerlo. Sin embargo, *The Guardian* ya publicó[284] con anterioridad informaciones acerca de la cooperación entre la

nearly everything", op. cit.

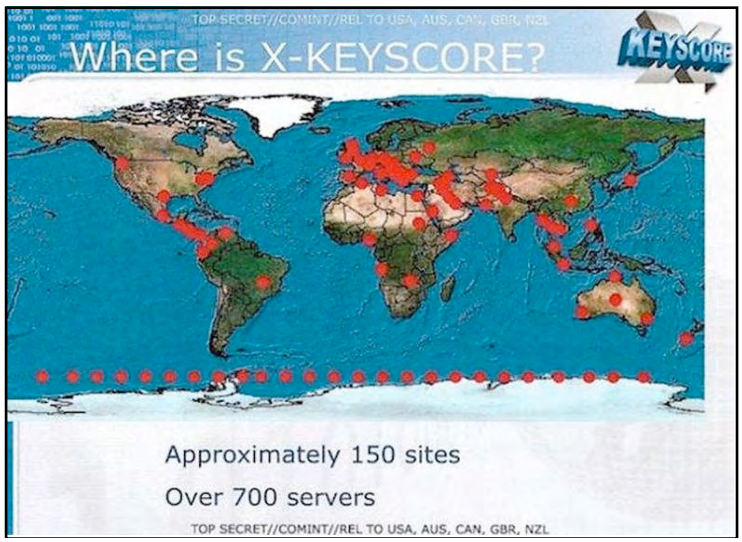
280 Fundado al amparo de la guerra de inteligencia protagonizada durante la II Guerra Mundial, con centro neurálgico en Bletchley Park, donde se llevarían a cabo los desciframientos del código Enigma empleado por la Alemania Nazi, el *GCHQ*, anteriormente conocido como *GC&CS* (*Government Code and Cypher School*) se constituyó tempranamente en un organismo de señales de inteligencia al margen de los otros dos servicios de inteligencia británicos: *MI5* y *MI6*.

281 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 118.

282 BALL, James, & BORGER, Julian, & GREENWALD, Glenn: "Revealed: how US and UK spy agencies defeat internet privacy and security", September 6, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

283 Ibíd.

284 Greenwald, Glenn & MacAskill, Ewen & Poitras, Laura & Ackerman, Spencer & Rushe, Dominic: "Microsoft handed the NSA access to encrypted messages", July 12, 2013, *The Guardian*, en: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p.6 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01d9/b8e19abe.dir/doc.pdf

*NSA* y *Microsoft* para eludir el cifrado en el servicio de correo electrónico *Outlook.com*.

## 5.8. Programas Upstream Collection.

A pesar del parecido con *PRISM*, dado que todos ellos son competencia de la *SSO*, los programas *Upstream Collection* impulsados por la *NSA,* basan su eficacia en los acuerdos contraídos con las compañías de telecomunicaciones asociadas a la hora de filtrar datos y metadatos tanto *DNR* como *DNI*, de ciudadanos, compañías e instituciones en el territorio. Registros todos ellos, no transmitidos por las propias compañías nacionales desde sus servidores, sino transferidos por el agente que sirve de puente, generalmente otra compañía de telecomunicaciones norteamericana, por medio de la disposición de infraestructura de cableados de comunicación submarinos. En una de las diapositivas reveladas, se diferencia claramente entre *PRISM* y *Upstream*, aunque se incita a los analistas a hacer uso de los dos medios.

En otra instantánea se pueden observar las redes de cableado submarino que constituyen la zona de tránsito autorizado para la recopilación de datos por la *NSA*.

Gracias a un memorándum de 2011 del juez John D. Bates, del *United States Foreign Intelligence Surveillance Court*, se conoció la capacidad de recolección de datos[285] por medio del sistema *Upstream* y bajo el amparo de la sección 702 de la *FISA Amendments Act* de 2008. Concretamente, la *NSA* interceptaba un total de 250 millones de comunicaciones por Internet cada año, de los cuales un 9% (22 millones) correspondían al sistema *Upstream* y el 92% restante (227 millones) al programa *PRISM*.

Los programas que forman parte del sistema *Upstream* son: *STORMBREW*, *BLARNEY*, *OAKSTAR* y *FAIRVIEW*.

### 5.8.1. Programa STORMBREW.

Según la documentación aportada por Snowden, *STORMBREW* es un programa dirigido en estrecha relación con el *FBI* y que otorga a la *NSA* acceso a Internet y al tráfico telefónico que entra en suelo norteamericano por varios cuellos de botella. Para Greenwald, "*el programa gestiona también dos puntos de conexión terrestre del cable submarino: uno en la costa oeste de EUU (BRECKENBRIDGE) y otro en la costa este (QUAILCREEK)*".[286]

285 BATES, D. John: *Memorandum Opinion*, United States Foreign Intelligence Surveillance Court, Washington DC, October 3, 2011, p.71, en: https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf

286 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 133.

Tal como se observa en las diapositivas reveladas, el programa dispone de siete accesos de información por los que se produce el tránsito tanto de registros *DNR* como *DNI*, bajo lo que se considera como un circuito de infraestructura doméstica de cables interconectados que abarca todo Estados Unidos. Los datos entran en la zona oeste del país por el punto de acceso con nombre en clave *BRECKENBRIDGE* y recorre los pasos de cables centrales conocidos como: *TAHOE*, *SUNVALLEY* y *WHISTLER* (que filtran la información obtenida de los cables submarinos que transitan por los océanos pacífico e índico y que conectan Oriente con Estados Unidos), y *MAVERICK*, *COPPERMOUNTAIN* y *KILLINGTON* (que filtran los datos procedentes de los cables submarinos en el océano atlántico y conectan Centroamérica, América Latina, y los continentes africano y europeo con las estaciones de Estados Unidos).

En un documento clasificado, revelado entre las filtraciones y con fecha del 19 de noviembre de 2003, bajo el titular: "*FAIRVIEW y STORMBREW: en vivo – en la red*", la *SSO* se jacta de que, al poco de su puesta en marcha, estos programas, consiguieron en un esfuerzo por modernizar las tareas de registros *DNR* y *DNI*, hasta cuadriplicar[287] la producción de señales *SIGINT*. De la misma forma, se reconoce la gran prestación de *STORMBREW* al dotarse de una Capacidad de Reacción Rápida (*QRC: Quick Reaction Capability*) la misma de que disponen todos los sistemas de recogida empleados por la *NSA* y que han prestado un apoyo esencial en la Guerra Global contra el Terrorismo.

En el mismo documento, se enuncia la estrecha colaboración entre los analistas que trabajan con la herramienta *FAIRVIEW*[288] y *STORMBREW* con el Centro de Análisis de Redes, para fomentar la explotación de los metadatos recogidos, la mejora de los filtros y selectores y la localización eficaz de los objetivos potenciales.

### 5.8.2. Programa OAKSTAR.

Según Greenwald, el programa *OAKSTAR* aprovecha el acceso de uno de los socios corporativos de la Agencia (nombre en clave *STEELKNIGHT*) a los sistemas extranjeros de telecomunicaciones, empleando este acceso para desviar datos a sus propios almacenes. Mientras, otro socio, "*(nombre en clave: SILVERZEPHYR) aparece en un documento del 11 de noviembre de 2009 que describe la labor realizada con la empresa para obtener "comunicaciones internas" de Brasil y Colombia*".[289]

*SILVERZEPHYR*, en tanto que socio del programa, permite recoger tanto registros *DNR* como *DNI*, gracias al punto de acceso a la red que menciona Greenwald, proporcionado por el socio comercial con nombre en clave *STEELKNIGHT*. A la vez, se identifican las zonas preferentes de recogida de datos y metadatos, y que son Centro América y América Latina.

El programa *OAKSTAR* cuenta a su vez con un conjunto amplio de subprogramas. Estos son: *MONKEYROCKET* (orientado a Europa, especialmente del este y Asia), *SHIFTINGSHADOW* (orientado a las comunicaciones afganas, especialmente las generadas por *MTN Group, Roshan telecommunications* y *GSM -Global System for Mobile Communications-*) *ORANGECRUSH*, *YACHTSHOP*, *ORANGEBLOSSOM*, *BLUEZEPHYR* y *COBALTFALCON*.

En un documento revelado, recogido por Greenwald, se establece la participación del Gobierno de Polonia[290] como intermediario para facilitar el envío masivo de datos bajo la herramienta

287 Special Source Operations: *FAIRVIEW and STORMBREW: 'Live' - On the Net*, Dynamic page – Highest possible classification is TOP SECRET, November 19, 2003.
288 Ibíd. 73

289 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 131.
290 Greenwald indica cómo *OAKSTAR*, bajo la cartera empresarial de las *SSO*, comenzó a enviar metadatos desde una página web de un tercero (Polonia) a depósitos de la *NSA* desde el 3 de marzo, y contenidos desde el 25 de marzo.

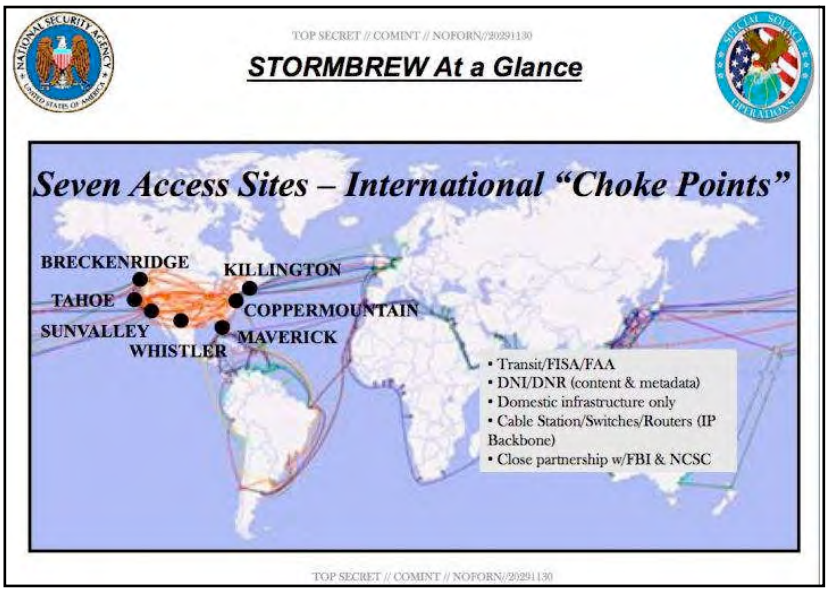
Fuente: Greenwald, Snowden: Sin un lugar donde esconderse, p.134.

Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 38
https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf

*ORANGECRUSH*, con origen en marzo de 2009, aunque el servicio de inteligencia polaco lo conoce bajo el nombre en clave *BUFFALOGREEN*. Al mismo tiempo, el documento establece el gran paso adelante en la recolección de metadatos que va a significar el subprograma, gracias siempre a los enlaces comerciales gestionados por el socio corporativo de la *NSA*, y se prevé que incluya "*comunicaciones del ejército nacional afgano, Oriente Medio, parte del continente africano y Europa. Se ha mandado una notificación a SPRINGRAY; esta recopilación está disponible para segundas partes a través de TICKETWINDOW*".[291]

En otro documento de alto secreto, con fecha de jueves 5 de septiembre de 2011, se confirma que *SILVERZEPHYR* suministra recopilaciones *DNR* en flujo permanente y *DNI* con la colaboración del socio, persiguiendo una cifra cercana a 80 *Gigabytes* de datos en sus redes interpares, lo que facilita la obtención de información de forma ins-

291 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 131.




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 23 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf

tantánea desde cualquier lugar del mundo[292] donde opere el programa.

### 5.8.3. Programa BLARNEY.

El programa *BLARNEY* es en realidad una versión[293] de *PRISM*. La diferencia esencial estriba en la ausencia de múltiples operadores con los que colabora este último, para confiar la transmisión de los datos de sus clientes en una sola compañía aliada: *AT&T*. Especialmente tras la absorción en 2005 de *SBC Communications*, su principal competidora, lo que hizo que se expandiera la cuota de mercado del Grupo, la encargada de las telecomunicaciones, según Greenwald, posibilitó de acuerdo con los archivos de la *NSA* "*en 2010 una lista de países seleccionados por BLARNEY que incluía Brasil, Alemania, Grecia, Israel, Italia, Japón, México, Corea del Sur y Venezuela así como la Unión Europea y las Naciones Unidas*".[294]

En una de las instantáneas filtradas sobre la funcionalidad de *BLARNEY*, se constatan desde el origen del mismo (en 1978 para proveer al Tribunal *FISA* acceso a comunicaciones de compañías extranjeras, agentes de potencias rivales y terroristas) al tipo de información obtenida (tanto registros *DNR* como *DNI* mediante órdenes *FISA*), los clientes del producto final obtenido (Casa Blanca, la *CIA* o los Departamentos de Estado o Seguridad Nacional son sólo algunos de ellos), los objetivos (las actividades de contraterrorismo, embajadas o consulados diplomáticos y las intenciones de las Naciones) y sus aliados (como la propia *NSA*, el *FBI* o el Departamento de Justicia y proveedores comerciales).

Gracias a su colaboración con *AT&T*, *BLARNEY* dispone de más de 70 accesos a los registros a lo largo de todo el territorio norteamericano, con el apoyo de más de 30 proveedores que actúan como socios corporativos internos para facilitar el acceso a cables de larga distancia nacionales como: *ARTIFICE*, *LITHIUM*, *ROCKSALT* o *SERENADE*. Para que la fluctuación de datos sea la más coherente, *BLARNEY* emplea la misma disposición de filtrado de información al paso de los cables por las estaciones, que utiliza el programa *STORMBREW*, mientras que las operatividades a disposición de los analistas se procesan en los dos grandes centros de datos ubicados en Washington D.C. y New York.

292 *OAKSTAR también está colaborando con NSAT para examinar instantáneas tomadas por el socio en Brasil y Colombia, que quizá contengan comunicaciones internas de esos países*. Ibíd.
293 Se trata de la versión internacional de *PRISM*.
294 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 129.

Ya en el año 2005, el ex técnico de *AT&T*, Mark Klein, testigo clave en la demanda colectiva que presentó *Electronic Frontier Foundation* en contra de la compañía, alegó la cooperación ilegal entre *AT&T* y la *NSA*, en base a la disposición de un engranaje de vigilancia para espiar el tráfico de Internet. El entramado, sobre todo, respondía a la conocida como estructura del "*secret room,*" que era la plataforma *Narus STA 6400*.[295]

### 5.8.4. Programa FAIRVIEW.

Para Thomas Drake, ex alto cargo de la *National Security Agency*, *FAIRVIEW* es el proyecto de la *NSA* para convertirse en el dueño de Internet, además de servir de paraguas para el resto de los programas *Upstream*: *STORMBREW*, *OAKSTAR* y *BLARNEY*. Centrado tanto en la recogida de mensajes como de llamadas telefónicas gracias a los sistemas de fibra óptica de los cables submarinos, que facilitan el tránsito e intercambio de información global. Según Greenwald, *FAIRVIEW* recoge de esta forma, enormes cantidades de datos de todo el mundo. "*Y se basa en un solo socio empresarial y concretamente en el acceso de este a los sistemas de telecomunicaciones de países extranjeros. Se trata de uno de los proveedores de metadatos más importante*".[296]

En la edición del 7 de julio de 2013 del diario brasileño *O Globo*, el propio Greenwald, en colaboración con los también periodistas Roberto Kaz y José Casado, revelaban a la opinión pública los entresijos del programa *FAIRVIEW* bajo el titular: "*Estados Unidos espía millones de emails y llamadas telefónicas de brasileños*".[297]En la información se destacaba que, en el mes de enero del mismo año, Brasil se convirtió en uno de los países más espiados por la *NSA* tras los Estados Unidos, con un registro total de cerca de 2,3 millones de llamadas y correos espiados.

Junto con países como China, Rusia, Irán o Pakistán, Brasil cuenta con una amplia red de sociedad digitalizada, y a la vez, con un entramado de compañías operadoras de telecomunicaciones, eminentemente privadas, lo que sin duda, supone un factor de atracción en la recopilación de datos por la *NSA*. Ahí es donde entra en juego *FAIRVIEW*, un programa que precisa de la cooperación de importantes empresas de telecomunicación, para conseguir colmar sus expectativas de alcance, y que cuenta con el apoyo de un socio corporativo de telefonía móvil de Estados Unidos para acabar creando una alianza corporativa mundial fuera de las fronteras del país.

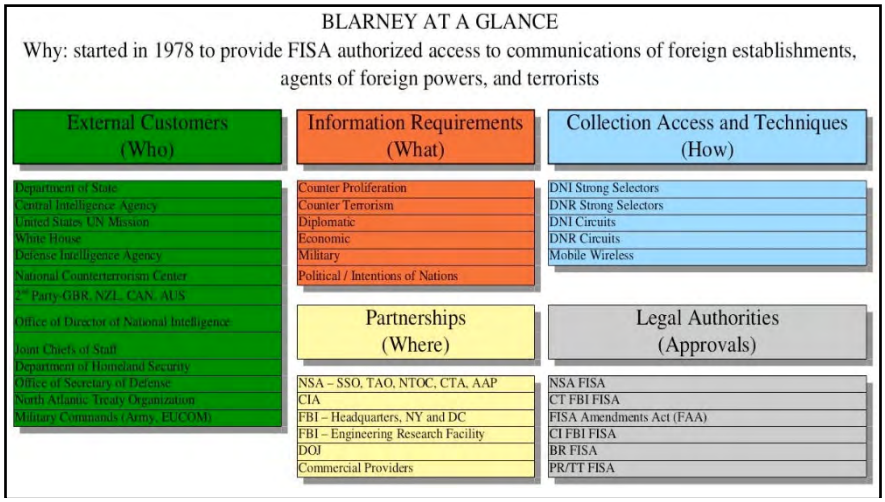
A pesar de que existan dudas de hasta qué punto las compañías brasileñas asociadas con la compañía estadounidense, que sirve de puente a la *NSA*, son conocedoras de cómo se utiliza dicha asociación, lo que está claro, según señala la publicación de *O Globo*, es que la *NSA* emplea *FAIRVIEW* para acceder directamente a los registros de la sociedad civil brasileña, compañías e instituciones, igual que ocurre con los diferentes lugares del mundo donde la compañía puente pueda tener los mismos lazos. En una de las diapositivas filtradas por Snowden, relativas al programa *FAIRVIEW*, aunque no se llega a identificar al socio corporativo que nutre de información a la herramienta, sí que se reconoce por la Agencia, la capacidad del mismo de acceder mediante sus relaciones con otras empresas de otras naciones, a los datos *DNR* y *DNI* que pueda generar con su actividad cualquier ciudadano.

Los datos obtenidos mediante la asociación empresarial en otro Estado, son enviados a las oficinas de procesamiento en Estados Unidos, mediante la

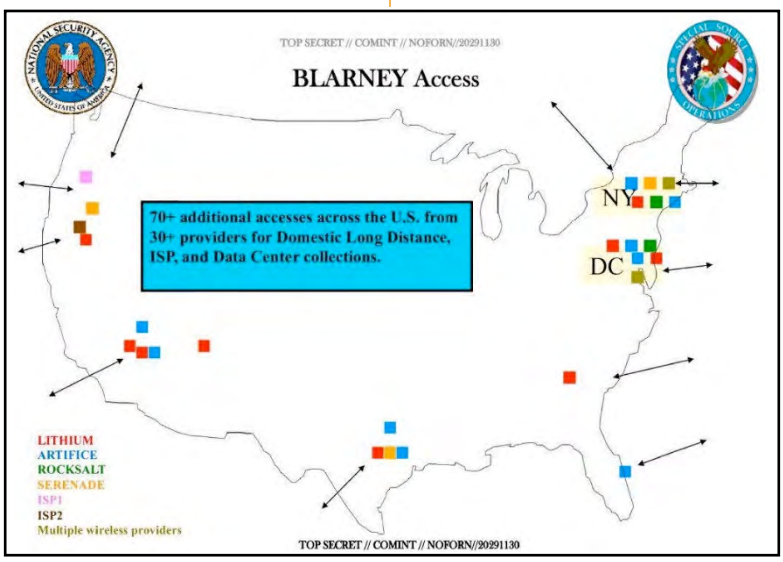
295 Un software en activo desde 1997, que constaba de analizadores del tráfico de Internet capaces de recoger el material de datos en bruto en tiempo real y transformarlo en unidades procesables gracias a su sistema de Análisis Semántico de Tráfico (*AST*).

296 Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 129.

297 GREENWALD, Glenn, & KAZ, Roberto & CASADO, José: "US spied on millions of emails and Brazilian bonds", July 7, 2013, *O Globo*, en: http://translate.google.com.br/translate?sl=pt&tl=en&-js=n&prev=_t&hl=en&ie=UTF- 8&u=http%3A%2F%2Fo-globo.globo.com%2Fmundo%2Feua-espionaram-milhoes-de-mails-ligacoes-de- brasileiros-8940934&act=url




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 20 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 21 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf

disposición de los cables submarinos que interconectan las comunicaciones de todo el mundo y que en algún momento, todas ellas, por razones de infraestructura, pasan por territorio norteamericano.

Así, tras la recepción de las comunicaciones, la estación *PINECONE* es la encargada de centralizar el procesamiento de los datos recogidos en el marco de *FAIRVIEW*. Al mismo tiempo, como se observa en otra de las instantáneas reveladas, se puede observar la disposición de la tecnología electrónica de largo alcance *4EEES*, a lo largo de todo el territorio norteamericano, bajo el llamado instrumento *RIMROCK*, es decir, un proceso previo que persigue filtrar y hacer llegar la información lo antes posible a *PINECONE*.

De la misma forma, como se ha mencionado con anterioridad, *FAIRVIEW* comenzó a colaborar con la estructura del programa *STORMBREW* de cara a masificar la obtención de productos *SIGINT*, obteniendo unos resultados de los cuáles la *NSA* se jactaba en uno de los documentos de alto secreto, ofrecidos a la opinión pública. También confirma la colaboración con *BLARNEY* a la hora de obtener registros *DNI* sobre la reunión de la *ONU* que tuvo

lugar en abril de 2012 en New York, e incluso se hace eco de la reanudación, el 5 de agosto de 2001, del cable *CLIFFSIDE*,[298] dada su avería a consecuencia del terremoto acaecido en Japón el 11 de marzo del mismo año.

## 5.9. La Estrecha colaboración con el Government Communications Headquarters (GCHQ) británico.

Desde el impulso de la relación entre sus servicios de inteligencia a partir de la firma del Tratado *UKUSA* de 1946, el acercamiento del *GCHQ* británico a las actividades rutinarias de la inteligencia norteamericana ha sido constante, hasta el punto de poder calificar a esta Agencia como el principal aliado de la *NSA*, ubicado más allá de las fronteras nacionales, con instrumentos y programas de vigilancia incluso más intrusivos que los emprendidos por la propia *NSA*, como se verá a continuación.

Los documentos de alto secreto revelados por Snowden descubren la cooperación entre *NSA* y *GCHQ*, lo que ha comprometido las garantías que las empresas especializadas en Internet ofrecen a sus clientes, asegurando que sus comunicaciones, sean de la naturaleza que sean, serán indescifrables tanto para delincuentes como para Gobiernos. En su lugar, la garantía de privacidad ha dejado paso a una construcción permanente de puertas traseras, vulnerabilidades expresas, colocadas con el único fin de destruir la encriptación comercial y hacer de la red global un filtro de escrutinio.

### 5.9.1. Programa OPTIC NERVE.

La demostración de hasta qué punto actúa el *GCHQ* en ese escrutinio salió a la luz el 27 de febrero de 2014, momento en que los periodistas Spencer Ackerman y James Ball hicieron público en *The Guardian* la existencia de una red de vigilancia clandestina,[299] con el apoyo de la *NSA* y una activa participación del *GCHQ*, consistente en el almacenamiento de millones de imágenes de usuarios por medio del pinchazo en red, de las webcams de sus ordenadores. El programa respondía al nombre de *OPTIC NERVE*, uno de los programas de inteligencia pioneros en emplear tecnología biométrica.

Tan sólo en 2008, durante un período de seis meses, la Agencia recogió un material en bruto de imagen derivado de las cámaras web, cercano a los 1,8 millones de cuentas[300] de usuario únicas de *Yahoo!*,[301] a nivel mundial. En la misma publicación, los responsables de la plataforma condenaron[302] enérgicamente el programa, alegando no tener conocimiento o implicación con la recogida masiva de imágenes por reconocimiento facial. Por su parte, ni *GCHQ*[303] ni *NSA*,[304] reconocieron la existencia de

298 En el documento se recogen los daños registrados en el cable como consecuencia del terremoto: "La evaluación inicial de los daños en el cable ha causado la pérdida de recogida de hasta 275 circuitos de señales *DNR* y de hasta 55 circuitos de señales *DNI*".
Véase Canadian Journalists for Free Expression (*CJFE*), Snowden Archive, *FAIRVIEW: CLIFFSIDE Site - Collection Resumes After 5 Months*, August 23, 2011, en: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf

299 ACKERMAN, Spencer & BALL, James: "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", February 27, 2014, *The Guardian*, en: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam- images-internet-yahoo

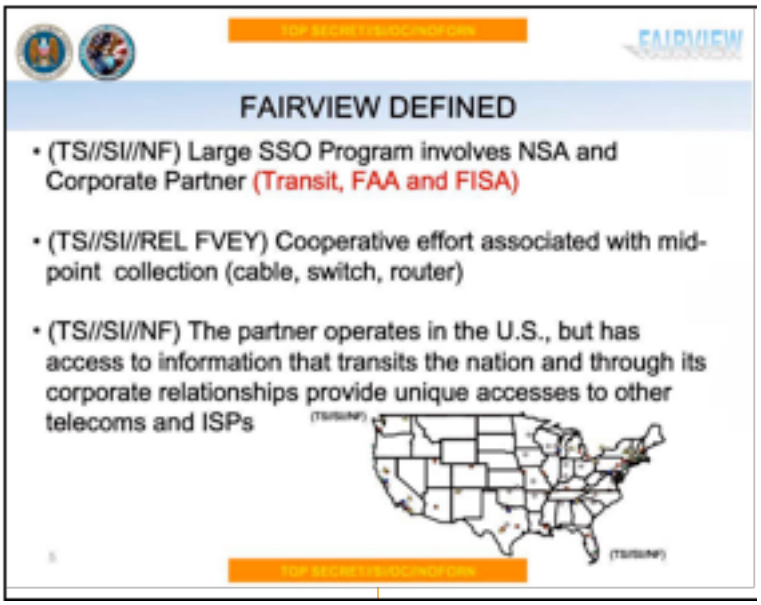
300 Ibíd.

301 Como señala el artículo, *OPTIC NERVE* se basa en la recogida de información de la red de cables de Internet, que luego se procesa y se introduce en los sistemas proporcionados por *NSA* y *GCHQ*. La herramienta de la *NSA*, *X- Keyscore*, llegó a ser utilizada por el *GCHQ* para la lectura biométrica de las imágenes captadas por webcam.
Ibíd.

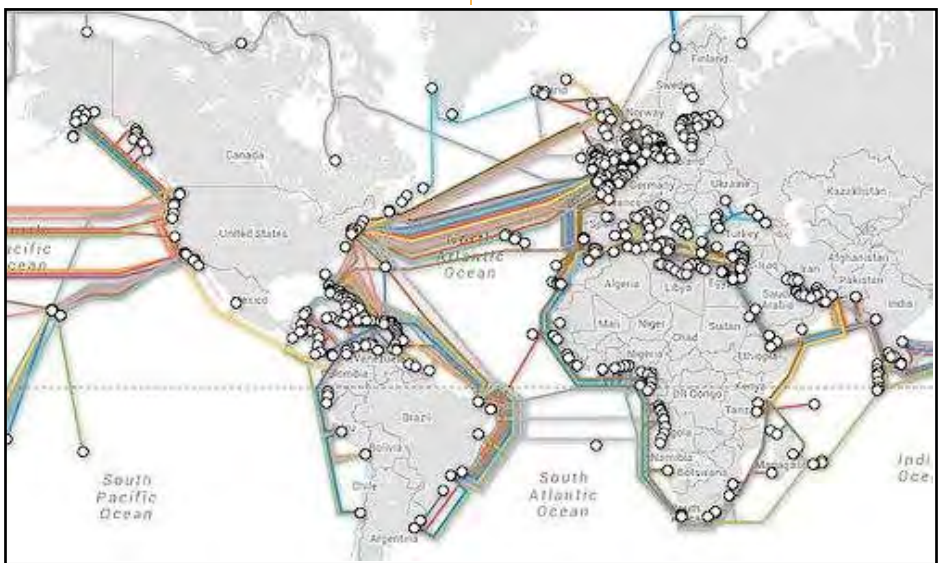
302 Un portavoz de la empresa *Yahoo!*, mostró el compromiso de la corporación con la seguridad y la privacidad de sus usuarios, mientras que hacía un llamamiento a reformar la Ley de vigilancia: "De ser cierto, estamos ante una violación de la privacidad de los usuarios, lo cual es inaceptable. Llamamos a los Gobiernos del mundo a la reforma de la Ley de vigilancia electrónica para que no se produzcan estas vulneraciones".

303 En un comunicado oficial, el portavoz del *GCHQ* dijo: "De acuerdo a nuestra política de actuación de largo recorrido en la Agencia, no hacemos comentarios sobre asuntos o temas de inteligencia".

304 Por su parte, la portavoz de la *NSA*, Vanee Vines, negó la colaboración con el *GCHQ* británico: "Como ya se ha dicho en otras ocasiones, la NSA no pide a sus socios extranjeros llevar cualquier tipo de actividad de inteligencia que el propio Gobierno de Estados Unidos tuviera prohibido y no estuviera legitimado a llevar a cabo".




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 40 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf




Fuente: TeleGeography/Submarine Cable Map http://www.submarinecablemap.com/

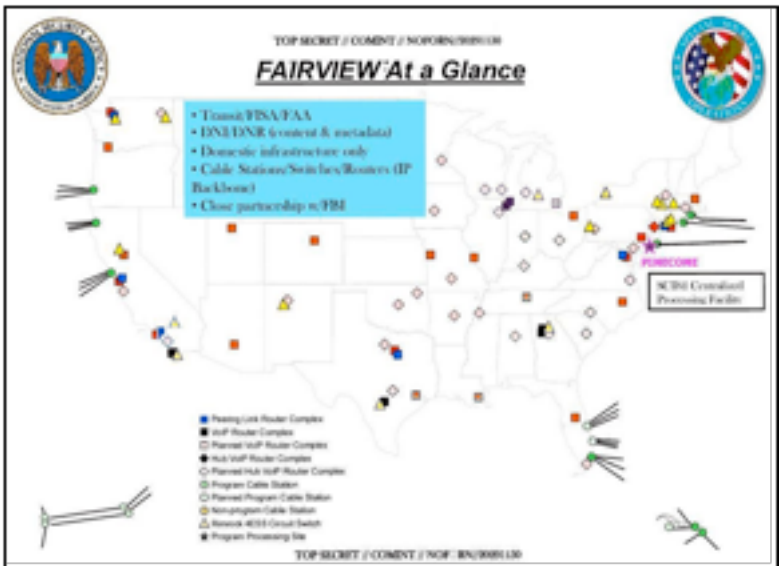
tal programa, a pesar de haber quedado revelado en la documentación filtrada.

Además de *OPTIC NERVE*, el *GCHQ*, en colaboración con la *NSA* ha emprendido varios proyectos para convertirse en protagonista del Estado de vigilancia global. Entre ellos, destacan *THIEVING MAGPIE* y *TEMPORA*.

### 5.9.2. Programa THIEVING MAGPIE.

Según Greenwald, en la reunión[305] de 2012 de

305 Un documento afín de la *NSA* presentado en la misma reunión, titulado "Homing Pigeon" (Paloma mensajera); también describe los esfuerzos para controlar las comunicaciones en el aire, en concreto coordinando el programa de la Agencia con el del *GCHQ* y haciendo que todo el programa esté disponible para el grupo de los Cinco Ojos.
Véase Greenwald, *Snowden: Sin un lugar donde esconderse*, op. cit., p. 207.




Fuente: Canadian Journalists for Free Expression/Snowdenarchive/ p. 22 https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f6/b9095c99.dir/doc.pdf

los Cinco Ojos, el *GCHQ* presentó un programa de interceptación denominado *THIEVING MAGPIE*, que se centraba en el creciente uso de teléfonos móviles durante los vuelos comerciales. "*La solución propuesta consistía en desarrollar un sistema que garantizase una cobertura completa. Se han hecho progresos sustanciales para garantizar que, en los aviones de pasajeros, ciertos dispositivos se prestan a la vigilancia*".[306]

Tal y como se observa en la documentación revelada, el programa perseguía poder acceder a los servicios móviles que cada vez se están ofreciendo más a los pasajeros entre las aerolíneas británicas. De esta manera, con la tecnología de *THIEVING MAGPIE* se había desarrollado la capacidad de seleccionar un objetivo en tiempo real y almacenar información personal relativa a emails o direcciones de Skype, con un rastreo autoejecutable con latencia de 2 minutos. Todo ello mientras el objetivo seguía en el vuelo.

Al mismo tiempo, con la aplicación de las prestaciones de *THIEVING MAGPIE*, la división de *Global Telecoms Exploitation* (*GTE*) del *GCHQ* se dedicó a explorar cómo acceder a aquéllos datos que los propios usuarios intentan proteger en *Facebook*, de modo que nada quedara fuera de su alcance. Como afirma Greenwald, "*En concreto el GCHQ ha observado, en el sistema de las redes de almacenamiento de imágenes, resquicios que pueden utilizarse para obtener acceso a cuentas de usuarios*".[307]

Tal y como se puede ver en la instantánea filtrada, el *GCHQ* insiste en que, mediante el acceso pasivo de la red social, se puede tener una puerta trasera abierta de forma permanente sin que el usuario sepa que la información oculta, no lo es tanto para la vigilancia de la Agencia, ni para la explotación o recolección de la misma.

### 5.9.3. Programa TEMPORA.

El *GCHQ* también ha realizado interceptaciones masivas de datos de comunicaciones por medio del empleo de cables submarinos de fibra óptica. Greenwald destaca las capacidades del programa llamado *TEMPORA* en la recopilación "*de actividad online, incluyendo registro de llamadas telefónicas, contenidos de mensajes de correo electrónico, entradas en Facebook o el historial de accesos a páginas web de cualquier usuario de internet*" y haciendo un especial hincapié en que "*las actividades de vigilan-*

306 Ibíd., pp: 205-206.

307 Ibíd., p. 202.

*cia del GCHQ son exactamente igual de exhaustivas– y tienen la misma patente de corso - que las de la NSA*".[308]

Con *TEMPORA*, el *GCHQ* tiene la capacidad para acceder a grandes cantidades de datos, extraídos de los cables de fibra óptica y almacenarlos durante 30 días, para que puedan ser cribados y analizados. Teniendo siempre en cuenta que, si bien la mayoría del flujo informativo o de datos, tanto *DNR* como *DNI* generados por los usuarios, en algún momento ha de pasar por los cables de Estados Unidos, en el continente europeo, ese papel lo ejerce el Reino Unido, concentrando la mayor presencia de cables[309] submarinos de fibra óptica de tránsito de datos, de todo el territorio europeo.

Con centros capaces de almacenar 10 *Gigabytes* por segundo, significa un acceso a aproximadamente, 21,6 *Petabytes* al día[310] de información recopilada por el *GCHQ* y por ende, dada su colaboración; por la *NSA*,[311]tanto de sospechosos identificados, como de personas totalmente inocentes, sin antecedentes criminales a su cargo. Snowden, quien llegó a exponer en los documentos filtrados a *The Guardian*, que el programa *TEMPORA* era, "*el mayor programa de vigilancia sin sospecha en la historia de la humanidad*",[312]ya reconocía el valor estratégico de la herramienta y su potencial, que confirió al *GCHQ* en 2010, a los dos años de su puesta en marcha, la capacidad de presumir de tener el acceso directo a internet, más grande de cualquier miembro de la alianza de espionaje de los Cinco Ojos. James Welch, Director de *Liberty*, ante la revelación del programa se preguntaba "*¿cuándo va a aprender [el Gobierno] que no es ni ético ni eficiente convertir a todos en sospechosos?*".[313]

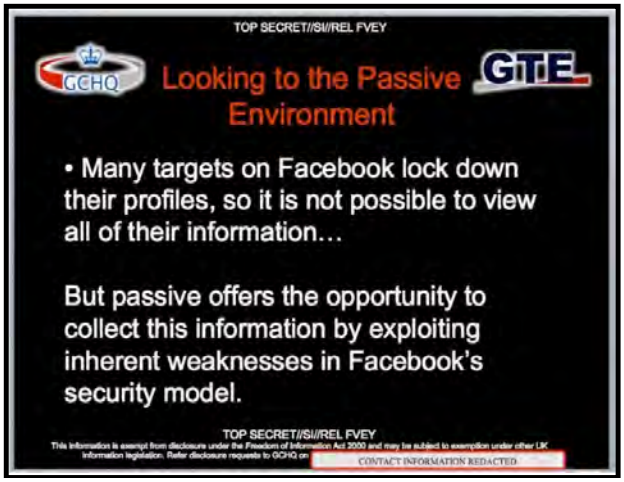
308 Ibíd., p. 149.
309 BUMP, Philip: "The UK Tempora Program Captures Vast Amounts of Data and Shares with NSA", June 21, 2013, *The Wire*, en: http://www.thewire.com/national/2013/06/uk-tempora-program/66490/
310 Una cantidad de información almacenada equivalente a 192 veces toda la colección de libros de la Biblioteca Británica.
311 Como se recoge en el artículo de Bump, entre ambas Agencias disponen de 550 analistas estudiando minuciosamente los datos y hasta 85.000 personas con autorización de alto secreto que pueden acceder a los mismos. Bump: "The UK Tempora Program", op. cit.
312 MACASKILL, Ewen, & BORGER, Julian, & HOPKINS, Nick, & DAVIES, Nick, & BALL, James: "GCHQ taps fibre-optic cables for secret access to world's communications", June 21, 2013, *The Guardian*, en: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
313 BOWCOTT, Owen: "GCHQ surveillance hearing to begin", July 14, 2014, *The Guardian*, en: http://www.theguardian.com/uk-news/2014/jul/14/court-gchq-surveillance-tempora-ipt-nsa-snowden

Fuente: Greenwald, Snowden: Sin un lugar donde esconderse, p.207.

## 6. Análisis de impacto de las revelaciones de Edward Snowden.

### 6.1. Ámbito interno de Estados Unidos.

Las revelaciones de Snowden abrieron un profundo debate en Estados Unidos, especialmente en lo que respecta al debate sobre los derechos a la privacidad de los ciudadanos norteamericanos. En general, la cobertura mediática fue muy crítica con las actividades de vigilancia de la *NSA*. Medios na-




Fuente: Greenwald, Snowden: Sin un lugar donde esconderse, p.202.

cionales como *The Washington Post*, *The New York Times*, *ProPublica* o *Mother Jones* publicaron editoriales en este sentido y mostraron los documentos que Snowden reveló al diario *The Guardian*. Del mismo modo, las revelaciones llevaron consigo numerosas protestas y campañas con objeto de detener los programas de la *NSA*. Así, eventos como "*StopWatching.US*" y "*The Day We Fight Back*", contaron con el respaldo de cientos de miles de ciudadanos [314]americanos que reclamaban la protección de la privacidad tanto de los estadounidenses como de los extranjeros residentes en Estados Unidos.[315]

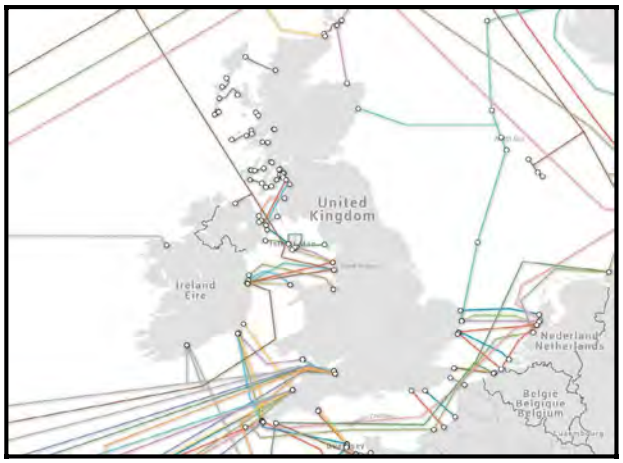
La respuesta legislativa vino de la mano de la *USA FREEDOM ACT*, que como ya se ha dicho, a pesar de la votación en contra del 22 de mayo de 2015, la propuesta fue aprobada justo un día antes de que finalizara la *USA PATRIOT ACT* de 2001, concretamente el 31 de mayo de 2015. No obstante, parece claro que la nueva Ley, en vez de regular los servicios de inteligencia y sus prácticas de vigilancia, se orienta más a ser el factor sustitutivo de la extinta *USA PATRIOT ACT*. Este hecho se observa si se atiende a que en la actual *USA FREEDOM ACT*, el Gobierno no está firmemente obligado a dar explicaciones sobre el grueso de población investigada bajo la Sección 215 durante más de una década, en el marco de la anterior Ley ni del número oficial de individuos investigados al amparo de la Sección 702 de la enmendada Ley *FISA*.

Además, es importante destacar que al menos seis casos judiciales fueron archivados poco después del escándalo en territorio norteamericano sobre la colección masiva de datos por la *NSA*. Ninguna de las demandas presentadas impugnaron la legalidad de los programas con respecto a la supervisión de civiles no estadounidenses.[316]

314 DAVIES, Simon: *A Crisis of Accountability. A global analysis of the impact of the Snowden revelations*, The Privacy Surgeon, published in association with Institute for Information Law and Law, Science, Technology & Society Studies, June 2004, p. 73.

315 Curiosamente si se observa el *Sandvine Global Internet Phenomena Report* correspondiente al primer año después de las revelaciones de Snowden, se percibe un denotado incremento en el tráfico de Internet encriptado. Véase *Sandvine Global Internet Phenomena Report*, 1H 2014, Canada, en: https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/2h-2014-global-internet- phenomena-report.pdf

316 Mientras las propuestas de reforma de la vigilancia se orientan a una mayor garantía de privacidad de los




Fuente: TeleGeography/Submarine Cable Map http://www.submarinecablemap.com/

A nivel ejecutivo, el Presidente Obama, como consecuencia del informe elaborado en diciembre de 2013 por un grupo de expertos sobre la legalidad de ciertos programas de vigilancia de la *NSA*, decidió dar luz verde a la Directiva presidencial número 28[317] orientada a instruir a la comunidad de inteligencia sobre las limitaciones en ciertas actividades de recolección y almacenamiento de datos. No obstante, y a pesar de que el Presidente indicó que propondría cambios en la legislación para la reforma de la vigilancia de la *NSA* y su supervisión eficaz por el Tribunal *FISA*, la propuesta específica aún no ha llegado.

## 6.2. Panorama internacional.

### 6.2.1. Naciones Unidas frente a los programas de la NSA. La acción diplomática de Brasil y Alemania.

El 26 de noviembre de 2013, el Tercer Comité de la Asamblea General de la *ONU* especializado en materia de asuntos humanitarios, sociales y culturales, impulsó una Resolución específica sobre el derecho a la privacidad. Aunque los grandes patrocinadores de la Resolución fueron Brasil y Alemania, cuyos Gobiernos y empresas transnacionales eran de las más circunscritas a la vigilancia de la *NSA*, un total de 55 países, incluidos Francia o Rusia, apoyaron la Resolución. Sometida a la votación de los 193 miembros de la Asamblea, el 18 de diciembre de 2013, la Resolución salió adelante.[318]

La Resolución, que hace mención al artículo 12 de la *Declaración Universal de los Derechos Humanos*[319] y al artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*,[320]como jurisprudencia de consolidación, reafirma "*el derecho humano a la intimidad, según el cual nadie será objeto de injerencias arbitrarias o ilegales en su vida privada , familia, domicilio o su correspondencia, y el derecho a la protección de la Ley contra tales injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para la realización del derecho a la libertad de expresión y para sostener opiniones sin interferencia, y es uno de los*

*cimientos de una sociedad democrática. Destacando la importancia del pleno respeto de la libertad de buscar, recibir y difundir información, incluyen-*

ciudadanos norteamericanos, desde el Gobierno no se hace mención alguna sobre modificaciones en el sistema de recolección de datos cuando se vean involucrados ciudadanos no estadounidenses.
Davies: *A Crisis of Accountability*, op. cit., p. 72.
317 Ibíd., op. cit., p. 73.

318 El embajador de Alemania ante la *ONU*, Peter Wittig, afirmó que la Resolución, pese a no ser vinculante, es un importante "mensaje político", pues constituye la primera vez que las *NNUU* afirman que la vigilancia doméstica y extraterritorial ilegal y arbitraria puede violar los derechos humanos. Por su parte, la delegada estadounidense, Elizabeth Cousens, afirmó que "Estados Unidos respeta y apoya la acción promovida por Brasil y Alemania" y se compromete en apoyar los derechos a la privacidad y el derecho a la libertad de expresión.
319 *Nadie podrá ser 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.*
Asamblea General de Naciones Unidas: *Declaración Universal de los Derechos Humanos*, Adoptada y proclamada por la Resolución de la Asamblea General 217, del 10 de Diciembre de 1948, Artículo 12, en: http://www.cnrha.msssi.gob.es/bioetica/pdf/declaracion_Univ_Derechos_Humanos.pdf
320 *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
Asamblea General de Naciones Unidas: *Pacto Internacional de Derechos Civiles y Políticos*, Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su Resolución 2200, de 16 de Diciembre de 1966, Artículo 17, en: http://www.migracion.gob.bo/web/upload/ddhh6.pdf

*do la importancia fundamental de acceso a la información y la participación democrática*".[321]

Al mismo tiempo, que exhorta a todos los Estados a respetar y proteger el derecho a la intimidad, incluso en el contexto de la comunicación digital, la Comunidad Internacional muestra en la Resolución su consternación y preocupación por el impacto negativo "*que la vigilancia y/o la interceptación de las comunicaciones, incluida la vigilancia extraterritorial y/o la interceptación de las comunicaciones, así como la recogida de datos personales, en particular cuando se lleva a cabo en una escala masiva, pueden tener sobre el ejercicio y disfrute de los derechos humanos*".[322]

Con la entrada en vigor de la Resolución a pesar de la falta de aplicación jurídica de las normas dictadas por la Asamblea General, la Alta Comisión de Derechos Humanos de las Naciones Unidas, ahonda en el conflicto al formular el 30 de junio de 2014, el primer informe sobre "*el derecho a la privacidad en la era digital*". En el mismo, la Comisión aduce a la necesidad de la vigilancia gubernamental al entender que "*los Gobiernos con frecuencia justifican los programas de vigilancia por motivos de seguridad nacional, incluyendo los riesgos planteados por el terrorismo. Varias contribuciones sugieren que, dado que las comunicaciones digitales pueden ser, y han sido, utilizadas por los objetivos criminales (para tareas como el reclutamiento o la financiación de actos terroristas), la vigilancia de la comunicación digital, puede constituir una medida necesaria y eficaz de inteligencia, siempre y cuando se lleve a cabo en cumplimiento de la legislación nacional e internacional*".[323]

Finalmente, entrado el año 2015, la Asamblea General impulsaría dos nuevas resoluciones en atención a las recomendaciones del informe elaborado por la Alta Comisión en Derechos Humanos y a la primera Resolución de 2014. De esta manera, el 10 de febrero de 2015, la Asamblea distingue, en una nueva Resolución, entre las prácticas ilícitas y aquellos objetivos legítimos a los que aludía la Comisión, además de incentivar a los Estados a que "*examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad,*"[324]tratando además de impulsar el reconocimiento de herramientas o recursos para las personas que hayan visto coartado tal derecho.

En la última Resolución emitida sobre este conflicto en el seno de la Comunidad Internacional, con fecha del 24 de marzo de 2015 y bajo el título "*El derecho a la privacidad en la era digital*", se reconoce la validez de los metadatos siguiendo criterios de seguridad nacional, pero señalando que "*algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona, poniendo de relieve que los Estados deben respetar las obligaciones internacionales de derechos humanos en lo referente al derecho a la privacidad cuando intercepten las comunicaciones digitales de las personas o reúnan datos personales y cuando exijan a terceros, incluidas las empresas privadas, la divulgación de datos personales*".[325]

321 United Nations, General Assembly: *Resolution adopted by the General Assembly* on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)], Sixty-eighth session A/RES/68/167, January 21, 2014, en: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

322 Ibíd.

323 Human Rights Council: *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, Twenty-seventh session. A/HRC/27/37, June 30, 2014, en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

324 Naciones Unidas, Asamblea General: *Resolución aprobada por la Asamblea General* el 18 de Diciembre de 2014 [sobre la base del informe de la Tercera Comisión (A/69/488/Add.2 y Corr.1)], Sexagésimo noveno período de sesiones A/RES/69/166, Febrero 10, 2015, en: http://www.un.org/es/comun/docs/?symbol=A/RES/69/166

325 Consejo de Derechos Humanos: *El derecho a la privacidad en la era digital*, 28º período de sesiones A/HRC/28/L.27, Naciones Unidas, Asamblea General, Marzo 24, 2015, en: http://ap.ohchr.org/documents/S/

Debido a la falta de carácter vinculante en lo que se refiere a la normativa dispuesta por la Asamblea General de la *ONU*, el Estado de vigilancia encuentra una mera fuente de rechazo de la Comunidad Internacional, como una especie de toque sincero de atención, sin que ello quiera decir que, pragmáticamente, la nueva base jurídica evite que los responsables sigan ejerciendo tales excesos.

### 6.2.2. El Parlamento Europeo: Comisión de Libertades Civiles, Justicia y Asuntos de Interior. [21/02/14]

Una de las esferas internacionales que hizo mayoritariamente palpable su malestar respecto a las técnicas de espionaje de la *NSA* en colaboración con otras Agencias y corporaciones transnacionales, fue el Parlamento Europeo. Desde que Snowden iniciara la batería de revelaciones a los periodistas de *The Guardian* en junio de 2013, diferentes sectores de la Eurocámara dejaron sentir su preocupación acerca de las conversaciones o embajadas diplomáticas europeas que habían sido cercadas por el escrutinio de los programas de inteligencia.

Aprovechando la coyuntura abierta por el Presidente Obama el 17 de enero de 2014, en cuyo discurso se recogía la ambivalencia de la ambición de reformar los excesos de espionaje, iniciados en la era Bush, junto con una defensa acérrima del trabajo de los analistas, el Parlamento solicitó a la *Comisión de Libertades Civiles, Justicia y Asuntos de Interior* la redacción de un informe titulado: "*Sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior*".[326]El 21 de febrero de 2014 se hizo público.

Las revelaciones, afirma el documento, han minado gravemente la confianza transatlántica[327] y han afectado negativamente en la confianza de cara a las organizaciones estadounidenses que operan en la UE; además de solicitar al Gobierno norteamericano, que fuera de juegos en la clandestinidad "*envíe señales políticas para demostrar que distinguen entre aliados y enemigos*".[328]

Asimismo, supedita las capacidades y poderes de los servicios de inteligencia a la estructura democrática y la justicia,[329]encargadas ambas de conferírselos, e involucra, sin duda, en las actividades de vigilancia, el papel activo que ejercen los Cinco Ojos, afirmando que las Agencias de seguridad nacional de Nueva Zelanda, Canadá y Australia "*pueden haber intercambiado recíprocamente datos personales de ciudadanos de la UE transferidos desde la UE*".[330]

### 6.2.3. Reacciones por países: **Alemania**.

Las filtraciones de Snowden en Alemania se dieron a conocer en el contexto de la campaña electoral de cara a las elecciones federales de septiembre de

HRC/d_res_dec/A_HRC_28_L27.pdf

326 Parlamento Europeo. Comisión de Libertades Civiles, Justicia y Asuntos de Interior: Documento de sesión. *Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior*, (2013/2188(INI)), A7-0139/2014, Febrero 21, 2014, en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7- 2014-0139+0+DOC+PDF+V0//ES

327 El documento señala que la crisis de confianza se extiende al espíritu de cooperación dentro de la UE, el respeto de los derechos fundamentales, la democracia y el Estado de Derecho, así como la credibilidad de las salvaguardas y el control democráticos, jurídicos y parlamentarios. Pero ante todo a los ciudadanos, quienes se dan cuenta de que ya no solo terceros países o multinacionales pueden estar espiándolos, sino que también sus propios Gobiernos, pueden estar haciéndolo.

328 Parlamento Europeo. Comisión de Libertades Civiles. *Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU*, op. cit., p. 45.

329 *Los servicios de inteligencia en las sociedades democráticas se les conceden poderes y capacidades especiales para proteger los derechos fundamentales, la democracia y el Estado de Derecho, […] que se deben utilizar dentro de los límites legales impuestos por los derechos fundamentales, la democracia y el Estado de Derecho y cuya aplicación debe someterse a un escrutinio estricto, ya que, de lo contrario, pierden legitimidad y pudieran socavar la democracia.*
Ibíd., p. 21.

330 Ibíd., p. 16.

2013. El impacto mediático fue relevante dado que todos los canales de televisión, tanto privados como públicos así como los periódicos más importantes, tanto en su edición impresa como online (*Spiegel*, *FAZ*, *Süddeutsche*

*Zeitung*, *Zeit*, *ZDF*, *ARD*, *RTL*, etc.) informaron ampliamente sobre las revelaciones del ex analista de la *NSA*.[331]

Después de promover junto a Brasil en noviembre de 2013, la Resolución específica sobre el derecho a la privacidad en el seno de la *ONU*, y especialmente preocupado por las revelaciones diplomáticas que involucraban actos de espionaje a la Canciller Angela Merkel,[332]el Bundestag estableció una Comisión de investigación sobre la *NSA* el 20 de marzo de 2014, inició su labor en abril y tiene una duración prevista de aproximadamente tres años.

Del mismo modo, organizaciones vinculadas a la sociedad civil[333] como *Reporters Without Borders Germany*, *Human Rights Watch*, *Whistleblower Netzwerk* o *Digitale Gesellschaft* pidieron al Gobierno alemán y al Bundestag intensificar la investigación y denunciaron la falta de transparencia del proceso, especialmente cuando el servicio de inteligencia exterior alemán, el *BND*,[334]se vio salpicado por el escándalo.[335]Actualmente continúa desarrollándose el trabajo de la Comisión.

**Australia**.

Las revelaciones de Snowden han afectado a Australia en la medida en que se trata de uno de los países que conforman el Club de los Cinco Ojos. La Agencia especializada en inteligencia electrónica en Australia es el *DSD*.[336]Entre los documentos que salieron a la luz se observa la cooperación[337] entre la *NSA* y el *DSD* orientada al intercambio de información especialmente de las regiones de Timor oriental, Malasia, Filipinas e Indonesia,[338]sin embargo, la revelación más impactante proviene de un documento filtrado con fecha de 2008, en el que el *DSD* se comprometió a facilitar a sus socios del Club, información confidencial de los ciudadanos australianos, hecho que según el abogado especializado en derechos humanos Geoffrey Robertson, vulnera la *Intelligence Services Act* de 2001.[339]Tras la revisión de la *Telecommunications (Interception and Access)*

331 DAVIES, Simon: *A Crisis of Accountability. A global analysis of the impact of the Snowden revelations*, The Privacy Surgeon, published in association with Institute for Information Law and Law, Science, Technology & Society Studies, June 2004, p. 42.

332 El 23 de octubre de 2013, el portavoz del Gobierno alemán, Steffen Seibert, afirmó que Berlín tenía información de que el teléfono móvil de Angela Merkel probablemente había sido espiado por Washington. El periódico *Die Welt* ofreció más información al asegurar que entre los documentos revelados por Snowden se encontraba el número de teléfono de la Canciller, con lo que existía la probabilidad de que la *NSA* hubiera intervenido las comunicaciones desde 2009. El 12 de junio de 2015, la justicia alemana cerró la investigación sobre las escuchas a Merkel alegando falta de pruebas.

333 En el otoño de 2013, *Freiheit statt Angst* (Libertad en vez de miedo) fue el lema de las manifestaciones en contra de la vigilancia estatal que tuvieron lugar en Berlín y lograron reunir a entre 10.000 y 15.000 personas.

334 *Bundesnachrichtendienst*.

335 En una entrevista al semanario *Der Spiegel*, Snowden acusó a la *NSA* de mantener relaciones estrechas con el *BND* alemán. La *NSA* se comprometió a facilitar el acceso a su programa *X-Keyscore* a la inteligencia alemana a cambio de que aportaran con regularidad registros de datos y metadatos obtenidos dentro del país.

336 *Defence Signals Directorate*. Hoy conocido como *Australian Signals Directorate* (*ASD*).

337 Davies: *A Crisis of Accountability*, op. cit., p. 15.

338 Por ejemplo, en el documento se recogen los intentos de la inteligencia australiana de escuchar las conversaciones telefónicas del Presidente de Indonesia, Susilo Bambang Yudhoyono, durante quince días de seguimiento en el año 2009. Véase: BRISSENDEN, Michael: "Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal", December 04, 2014, *ABC News*, en: http://www.abc.net.au/news/2013-11- 18/australia-spied-on-indonesian-president,-leaked-documents-reveal/5098860

339 Violaría las secciones 8 y 10 de la Ley, en las que se incide en el requisito de autorización ministerial si los datos de un ciudadano australiano están involucrados en las propias actividades de inteligencia. Para que un ciudadano australiano sea objetivo de inteligencia, según la Ley, debe tratarse de una "persona de interés", como alguien involucrado en el terrorismo o el crimen organizado. Act Nº: 152: *Intelligence Services Act 2001 Australia*, October 29, 2001.en: http://www.austlii.edu.au/au/legis/cth/consol_act/isa2001216/

*Act* de 1979 y de la *Privacy Act* de 1988,[340]con objeto de garantizar la privacidad de los ciudadanos frente a las actividades de vigilancia, persisten las dudas acerca de la capacidad de cerco a los servicios de inteligencia y la cooperación interdepartamental.

**Brasil**.

Después de conocerse los casos de espionaje a la Presidenta Dilma Roussef y a la empresa nacional de petróleo, Petrobrás, el Gobierno brasileño reaccionó en dos frentes: por un lado dio luz verde en septiembre de 2013 a la Comisión de Investigación Parlamentaria "*CPI da Espionagem*",[341]y por el otro cooperó a partir de noviembre del mismo año con Alemania en el impulso de la Resolución en la *ONU* sobre el derecho a la privacidad.

Por otro lado, como respuesta a la vigilancia de la *NSA*, en 2014 se impulsó el "*Marco Civil*",-[342]que obligaba a que cualquier operación respecto a la recopilación, almacenamiento y el tratamiento de comunicaciones de datos personales o por los ISP[343] que se producen en territorio brasileño "*deben respetar la legislación brasileña y los derechos a la intimidad, la protección de los datos personales y la confidencialidad de las comunicaciones privadas*".[344]El texto se aprobó en el marco de la *NetMundial*,[345]celebrada en Sao Paulo entre el 23 y 24 de abril de 2014.

**Canadá**.

Al igual que Australia, Canadá al formar parte del Club de los Cinco Ojos se ha visto implicado en las acusaciones sobre la cooperación entre la *NSA* y su servicio de inteligencia, el *CSEC*.[346]En respuesta a la vigilancia, tanto la sociedad civil como el sector académico canadiense han trabajado para poner en marcha la *Protect Our Privacy Coalition*,[347]como medida de presión hacia el Parlamento para frenar las actividades intrusivas del *CSEC*.

Además, la *British Columbia Civil Liberties Association* ha llevado a cabo una impugnación del marco legal en el que se amparan las actividades del *CSEC* al entender que infringe permanentemente las secciones 8 y 2 (b) de la *Canadian Charter of Rights and Freedoms*.[348]Del mismo modo, la *Canadian Civil Liberties Association*, también ha puesto en marcha una demanda para impugnar la

340 La *Australian Law Reform Commission* reconoció e incorporó a la *Privacy Act* de 1988, la violación de la intimidad de la persona como complemento de protección cuando la información personal sea utilizada y transferida entre terceros.
Véase Davies: *A Crisis of Accountability*, op. cit., p. 17.
341 Finalizada el 11 de abril de 2014, durante su investigación se llegó a plantear la idea de contactar con Snowden por videoconferencia e incluso desplazarse a Rusia para tratar de hablar con el ex analista de la *NSA* y esclarecer los actos de espionaje. No obstante, la embajada de Rusia en Brasil no llevó a cabo los procesos necesarios para que se produjera el encuentro. A pesar de exigir una mayor transparencia del Gobierno e inversión económica para combatir la contrainteligencia, la Comisión concluyó que Brasil no está preparado para garantizar una seguridad cibernética plena de sus ciudadanos a la vez que no fue capaz de encontrar a los culpables de las acusaciones de colaborar con la *NSA* en el país.
Véase Requerimento nº 811-2013, Portal Atividade Legislativa: *CPI da Espionagem* (*CPIDAESP*), 03 Septiembre, 2013, en: http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=&com=1682
342 Se trata de una legislación brasileña cuyo objetivo es introducir el respeto a los derechos civiles en el uso de Internet en Brasil.
343 *Internet service provider* (proveedor de servicios de Internet).
344 Davies: *A Crisis of Accountability*, op. cit., p. 19.
345 Una organización concebida tras las revelaciones de Snowden para reunir a diferentes grupos de interés, corporaciones empresariales y representantes de naciones y discutir la elaboración de principios universales que gestionen Internet a modo de hoja de ruta.
346 *Communications Security Establishment Canada*.
347 Compuesta por más de 50 grandes organizaciones y dos decenas de destacados académicos. Uno de los talleres generó la *Ottawa Statement on Mass Surveillance*, que persigue el refuerzo de la privacidad ciudadana frente a los abusos de Inteligencia.
Véase Davies: *A Crisis of Accountability*, op. cit., p. 22.
348 Que hacen referencia a la incautación irrazonable y a los derechos de libertad de pensamiento, creencia, opinión y expresión, incluida la libertad de prensa y de los medios de comunicación.
Véase British Columbia Civil Liberties Association, *Spying in Canada: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying on Canadians*, October 22, 2013, en: http://bccla.org/wp-content/uploads/2013/10/Final-Press-Release-Spying-10_21_131.pdf;

constitucionalidad de la *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[349]especialmente en lo relativo a la notificación obligatoria de las empresas a sus clientes cuando hayan entregado información confidencial a Agencias dependientes del Estado y que sirven al *CSEC* para labores de investigación.

**España**.

En el caso español, la primera reacción tras las revelaciones de Snowden[350] llegó de la mano de la Agencia Española para la Protección de Datos, que demandó a las autoridades de la Unión Europea un esfuerzo en la solicitud de información al Gobierno de Estados Unidos para aclarar el escándalo.

Una de la revelaciones más importantes fueron las ocurridas en noviembre de 2013, cuando algunos medios de comunicación españoles [351]revelaron que el Centro Nacional de Inteligencia de España habría facilitado a la *NSA* entre diciembre de 2012 y enero de 2013, registros de aproximadamente 60 millones de llamadas telefónicas de civiles españoles y extranjeros en suelo español.[352]Ya en marzo de 2014 en el marco de la Comisión *LIBE*[353] se publicó el informe *Electronic Mass Surveillance of EU Citizens*, que utilizó la oposición de izquierdas en el Congreso para preguntar qué medidas se habían adoptado por el Gobierno para cumplir las recomendaciones del informe. No obstante, a pesar de la indiferencia generalizada en los medios de comunicación españoles, el debate sobre la privacidad parece emerger con fuerza en la actualidad.[354]

**Francia**.

Tres semanas después de las primeras publicaciones sobre las revelaciones de Snowden en el semanario *Der Spiegel* y el diario *The Guardian* a mediados de junio de 2013, Laurent Fabius, ministro de asuntos exteriores francés, instó al Gobierno de Estados Unidos a realizar una explicación oficial.[355]

La única reacción parlamentaria en Francia tuvo lugar el 22 de mayo de 2014, momento en que se iniciaron las audiencias públicas de expertos en seguridad y derechos civiles en el marco de una conferencia conocida como "*Numérique, renseignement et vie privée: de nouveaux Défis pour le droit*". En cuanto al programa *PRISM*, la justicia francesa admitió a trámite la demanda interpuesta por la *Federación Internacional de Grupos de derechos humanos* (*FIDH*), en agosto de 2013, aunque todavía está pendiente la apertura de la investigación judicial. Por último, tanto en julio de 2013 como en marzo de 2014, se votaron e introdujeron en el sistema legal francés, medidas orientadas al "*geo-tracking*", es decir, a limitar la capacidad de las Agencias de vulnerar la privacidad debido a las prestaciones tecnológicas en favor de la localización de civiles por medio de sus teléfonos móviles.

349 Davies: *A Crisis of Accountability*, op. cit., p. 23.
350 En julio de 2013, tan solo un mes después de las primeras revelaciones al diario *The Guardian*, Edward Snowden solicitó el asilo al Gobierno español a través de la embajada de Moscú. El Gobierno denegó el asilo al tratarse de un trámite que el asilado debe realizar en suelo del país en el que solicitar asilarse, en aquel momento se encontraba en Hong Kong.
Véase Ibíd, op. cit., p. 67.
351 *El País* y *ElDiario.es* fueron los medios que se hicieron eco de las revelaciones.
352 Estas informaciones fueron negadas por el Director de la *NSA*, Keith Alexander, quien hizo hincapié en que los metadatos obtenidos se encuadraban en la colaboración regular de ambos países en la *OTAN* y que se referían únicamente a las actividades sospechosas en terceros países, esencialmente Mali y Afganistán.
353 La Comisión de Libertades Civiles, Justicia y Asuntos de Interior responsable de la protección, dentro del territorio de la Unión Europea, de los derechos de los ciudadanos, los derechos humanos y los derechos fundamentales.
354 Davies: *A Crisis of Accountability*, op. cit., p. 69.
355 El único gesto diplomático entre ambos países lo llevó a cabo el propio Fabius, quien el 21 de octubre de 2013 afirmó que había llamado al embajador de Estados Unidos para mantener una reunión. Este hecho se produjo el día en que el diario *Le Monde* publicó nuevos documentos revelados por Snowden sobre cómo de masivo fue el espionaje de la *NSA* y su impacto en los intereses geoestratégicos franceses.
Véase Ibíd., op. cit., p. 38.

**México**.

Las reacciones en México comenzaron a partir de septiembre de 2013, momento en que el periódico brasileño *O Globo* escribió,[356] sobre la base de los documentos confidenciales divulgados por Edward Snowden, acerca de cómo la *NSA* había intervenido ilegalmente las comunicaciones del entonces candidato a la presidencia de México, Enrique Peña Nieto.[357]

Al tener en cuenta de que se trataba de una intrusión en la soberanía de México, muchos congresistas condenaron el espionaje de la *NSA* y en julio de 2013 el Congreso adoptó una Resolución en contra de la vigilancia y cualquier tipo de práctica que violara el derecho a la privacidad de los ciudadanos mexicanos.[358] El 15 de enero de 2014, sin embargo, el Ministerio de Administración Pública firmó un contrato marco con empresas como *Google* y *Microsoft* hasta 2016 para la adquisición de licencias de software y a pesar de que tales empresas se encontraban en el centro de la diana.[359] Ya en mayo de 2014, el Ministerio del Interior desarrolló nuevas normas aplicables a todos los servicios encargados del almacenamiento y la gestión de datos de las instituciones públicas y el tratamiento de los datos sensibles de seguridad nacional, en virtud de un incremento de la seguridad de la información.[360]

De la misma manera, las ONG como *ContingenteMX* y *SonTusDatos* protagonizaron campañas[361] de movilización ciudadana en contra de los programas de vigilancia de la *NSA* activos en suelo mexicano. A pesar de la pasividad gubernamental con relación al espionaje de la *NSA*, las organizaciones civiles han sido las principales protagonistas de la reacción mexicana al escándalo.

**Reino Unido.**

Si algún Gobierno se ha visto involucrado en las revelaciones de Snowden junto con el Gobierno norteamericano, ese ha sido el británico. La cooperación en materia de vigilancia e intercambio de información entre el *GCHQ* y la *NSA* ha puesto de manifiesto la falta de control gubernamental sobre las Agencias de inteligencia británicas.[362] A pesar de que los lazos entre *NSA* y *GCHQ* van más allá de la colaboración integrada dentro del Club de los Cinco Ojos, por ejemplo participando en la puesta en marcha de programas como *THIEVING MAGPIE*, de cara al almacenamiento y escucha telefónica durante vuelos comerciales o *TEMPORA*, mediante la explotación de cables submarinos de fibra óptica, las reacciones gubernamentales han sido del todo laxas.[363]

356 TARDÁGUILA, C & GAMA, J: "EUA espionaram Dilma", September 01, 2013, *O Globo*, en: http://oglobo.globo.com/pais/eua-espionaram-dilma-9782118.

357 En octubre de 2013 el semanario alemán *Der Spiegel* publicó un informe en el que se informaba de la interceptación de los mensajes de correo electrónico tanto del ex Presidente de México, Felipe Calderón, como de la Oficina del Presidente, como parte de la operación "Flatliquid".

358 El partido político *PRD* solicitó que en la Resolución se incluyera una petición formal para emitir un informe que pidiera explicaciones al Gobierno norteamericano y se solicitara información sobre los acuerdos de cooperación entre Estados Unidos y corporaciones empresariales en territorio mexicano. Con el tiempo no se incluyó la petición. Véase Davies: *A Crisis of Accountability*, op. cit., p. 52.

359 Debido a las acusaciones debido a su cooperación con la *NSA*, a pesar de que sus portavoces negaron en reiteradas ocasiones la colaboración y acusaron a la Agencia de actuar a sus espaldas.

360 Davies: *A Crisis of Accountability*, op. cit., p. 53.

361 El 11 de febrero de 2014, las ONG como *ContingenteMx*, *SonTusDatos*, empresas como Mozilla y Wikimedia, así como sitios web de Internet, como *Nodo9* y *Sopitas* se unieron a la campaña internacional "The Day We Fight Back" para oponerse al espionaje de la *NSA*.

362 En gran parte amparadas por el Proyecto de Ley *Draft Communications Data*, también conocida como *Snoopers' Charter*, anunciada en 2013 y recuperada tras la victoria conservadora en mayo de 2015 por la ministra del interior Theresa May. Este Proyecto más allá de limitar, fortalece las prácticas actuales de las Agencias y supone requerir a proveedores de Internet y empresas de telefonía móvil la elaboración regular de un registro de cada usuario incluyendo las redes sociales, la correspondencia de correo electrónico, llamadas de voz y los servicios de mensajería, y almacenarlos durante 12 meses.

363 La sorpresa y la indignación mostrada por los políticos en el inicio de las filtraciones de Snowden, murieron

En la actualidad, las iniciativas[364] más prometedoras de reforma y control de las Agencias de inteligencia británicas han llegado de la mano de organizaciones como *Privacy International*, *Amnesty International*, *Bytes for All* (Pakistán), *Liberty*, o *ACLU*, entre otras, apelando al único Tribunal con capacidad de reforma de la comunidad de inteligencia británica, el *Investigatory Powers Tribunal*.[365]

**Rusia**.

Después de las revelaciones al diario *The Guardian* en Hong Kong, Snowden huyó hacia Rusia el 23 de junio de 2013 y tras pasar cinco semanas en la zona de tránsito del aeropuerto Sheremetievo de Moscú, finalmente el 1 de agosto de 2013, el Gobierno le concedió el derecho de asilo por un año.[366]El caso Snowden supone el punto más bajo en las relaciones diplomáticas entre ambos países, espiral que ya se inició en 2008 cuando estalló el conflicto armado en Osetia del sur entre Georgia, las repúblicas pro-rusas de Osetia del Sur y Abjasia y la misma Rusia. La imposición de Washington de fuertes sanciones a Moscú con objeto de proteger a su aliado estratégico en la región, Georgia, dio comienzo a un incremento de la tensión entre ambos países y a un relanzamiento de acuerdos bilaterales en materia de la no proliferación nuclear, lucha contra el terrorismo y la ciberseguridad.[367]

La invasión de Crimea en el marco de la crisis ucraniana de 2014,[368]no ha hecho sino distanciar aún más a los Gobiernos de ambas naciones. Tras la concesión de asilo, el propio Presidente Vladimir Putin, confiaba en que las relaciones diplomáticas entre ambos países no se vieran afectadas[369] puesto que el asilo de Snowden estaría sujeto a no revelar más secretos que pudieran afectar a los intereses de Estados Unidos. No obstante, la negativa a su extradición y la concesión el 1 de agosto de 2014 de un derecho de asilo prorrogado durante tres años más, han ayudado a generar un ambiente de desconfianza fundamentado en el riesgo de filtración de secretos norteamericanos de inteligencia al Gobierno ruso.

En la actualidad, el conflicto sirio también es foco de tensión entre ambos, después de que Rusia respalde la figura de Bashar al-Assad al frente del régimen, mientras que Estados Unidos es proclive de buscar una transición al régimen sin el causante de la propia guerra civil.[370]

## 6.3. Reacciones de otros observadores: Human Rights Watch y American Civil Liberties Union.

Entre los observadores globales que mostraron su criticismo de forma activa a la incentivación del Estado de vigilancia creado por las sofisticadas técnicas de espionaje, guarda un espacio relevante *Human Rights Watch* (*HRW*), organización no gubernamental dedicada específicamente a la protección

rápidamente. En la actualidad, los funcionarios encargados de supervisar el *MI5*, el *MI6* y el *GCHQ* rara vez aluden al intrusismo excesivo y dedican palabras en contra de la vigilancia británica.
Véase Davies: *A Crisis of Accountability*, op. cit., p. 70.

364 También se han llevado campañas por las organizaciones *Big Brother Watch*, *Open Rights Group*, *English PEN*, y la campaña de Internet *Constanze Kurz* han llegado incluso a impugnar la vulneración civil de derechos al Tribunal Europeo de Derechos Humanos.

365 Establecido por la Ley Regulation of Investigatory Powers del año 2000, su función es similar al Tribunal *FISA* en Estados Unidos y de igual manera, de forma tradicional tiende a emitir fallos favorecedores casi siempre del lado del Gobierno.

366 Tres países de América Latina: Venezuela, Nicaragua y Bolivia, mostraron su disposición a conceder asilo político al fugitivo una vez que Ecuador, país al que quiso viajar desde el primer momento Snowden, respondiera con más reservas a su petición de asilo.

367 WELT, Cory: *What the Snowden affair says about U.S.-Russian relations*, Center for American Progress, July 17 2013, p. 2, en: https://cdn.americanprogress.org/wp-content/uploads/2013/07/SnowdenAffair-brief1.pdf

368 Una crisis diplomática internacional que sobrevino tras el fin del Gobierno de Víktor Yanukóvich producto de las protestas del Euromaidán, iniciadas después de que el Gobierno de Ucrania suspendiera la firma del Acuerdo de Asociación y el Acuerdo de Libre Comercio con la Unión Europea.

369 NICHOL, Jim: *Russian political, economic, and security issues and U.S. interests*, Congressional Research Service, CRS Report, March 31, 2014, p. 55, en: https://www.fas.org/sgp/crs/row/RL33407.pdf

370 Welt: *What the Snowden affair says*, op. cit., p. 3.

de los derechos humanos. En dos de sus últimos informes mundiales, tanto el elaborado en relación al balance del ejercicio 2014, como en el de 2015, se hace notar la fuerte reacción frente al criterio de observación mundial de las comunicaciones. En el documento del año 2014, parte de la premisa legitimadora que confiere a los Gobiernos la protección de la seguridad nacional para ejecutar prácticas de vigilancia selectiva dentro de unos límites, aunque admite, "*la vigilancia masiva del Gobierno de Estados Unidos, sin este tipo de límites, en gran medida ha eliminado el derecho a la privacidad en una época donde la población prácticamente depende de la comunicación electrónica*".[371]

El observador atiende a que la promesa de la era digital es la capacidad espontánea y sin fronteras para compartir información, pero esa es al mismo tiempo su amenaza.[372]No obstante, el debate iniciado tras las filtraciones ha implicado la puesta en marcha de un reclamo fundamental, como es la reafirmación ciudadana en su derecho a la privacidad al insistir en que tal derecho, no es sólo una cuestión de dejar en paz a las personas, sino que consiste en "*una capacitación para que se conecten, hablen, piensen y vivan bajo sus propios términos, sin la arbitraria interferencia estatal*".[373]

Finalmente, *HRW*, alude a una necesaria respuesta compleja y global contra la vigilancia para recuperar el ciclo de la credibilidad y la confianza ciudadana, pero fundamentalmente señala al Gobierno norteamericano, toda vez que ostenta un papel clave en la cibertecnología mundial y es el responsable principal del espionaje global. En este sentido, como peticiones esenciales en su informe se requieren "*la protección del acceso a los metadatos con el requisito de una orden judicial, reconocer que la privacidad es violada cuando se recopilan los datos (y no sólo cuando se ven o se utilizan), modernizar la corte FISA para que sea un órgano más antagonista y transparente con el objetivo de supervisar la NSA y proteger a los informantes que revelan las prácticas de seguridad nacional que violan los derechos humanos*".[374]

En el informe del año 2015, *HRW* mostraba su contrariedad ante las declaraciones del Presidente Obama en enero de 2014, al entender que, a pesar de las medidas comprometidas para reformar la inteligencia, un elevado componente de vaguedad en las mismas, les hacía imposible ir más lejos a la hora de evitar el abuso "*y no crean derechos que las personas no estadounidenses pueden hacer valer ante los tribunales*".[375]Asimismo, el observador también incide en que, si bien la controversia de Snowden ha centrado el debate en los Gobiernos de Estados Unidos y Reino Unido, no hay ninguna razón para creer que las prácticas de otros Estados seanmejores.[376]

También es importante la mención que se hace al ámbito comercial, dado que a partir de 2014, tras las revelaciones de los excesos de la *NSA*, las principales empresas de tecnología estadounidenses[377] re-

371 Human Rights Watch: *Informe mundial 2014*, p. 13, en: http://www.hrw.org/sites/default/files/reports/wr-2014sp_web.pdf

372 *A medida que la información del mundo migra hacia el ciberespacio, las capacidades de vigilancia han crecido proporcionalmente. […] Al final, no habrá ningún refugio seguro si la privacidad es vista como una cuestión estrictamente nacional, sujeta a muchos diseños y una supervisión laxa o inexistente. […] La vigilancia masiva global representa una amenaza para los derechos humanos y la democracia, y una vez más, la Ley debe aceptar el reto.*
Ibíd., p. 18.

373 Ibíd., p. 27.

374 Ibíd., p. 25.

375 Human Rights Watch: *Informe mundial 2015*, p. 17, en: http://www.hrw.org/sites/default/files/wr2015_web.pdf

376 En este sentido, el informe incide en que la mayoría de las regulaciones sobre el derecho efectivo de privacidad, ya se pusieron en marcha durante la infancia de Internet, mucho antes de que existieran las redes sociales o los teléfonos inteligentes. No obstante, ahora parece que aquéllas regulaciones o protecciones, no sean suficientes y observamos cómo Gobiernos como Etiopía, China, o Rusia, habitualmente incluyen la vigilancia abusiva de las comunicaciones en sus políticas. Como señala el informe, se produce así el desigual progreso en el tiempo entre evolución tecnológica y regímenes de privacidad, hasta el punto de llegar a entender una relación inversa entre ambos.

377 *En septiembre de 2014, Google y Apple anunciaron que los datos almacenados en sus dispositivos móviles serán encripta-*

doblaron sus esfuerzos para fortalecer la seguridad de sus dispositivos contra el espionaje. No obstante, está por ver si tales empresas han ejercido un papel colaborador en el impulso de algunos de los programas de inteligencia y si verdaderamente son capaces de edificar una estructura de Internet al margen del Gobierno.

En su último informe de 2016, *HRW* señala cómo tanto John Brennan, Director de la *CIA*, como James Comey, del *FBI*, especialmente tras la secuencia de atentados en París de noviembre de 2015,[378]han reactivado los esfuerzos[379] para exigir a las grandes compañías de Internet el endurecimiento de sus infraestructuras, con objeto de que los terroristas no encuentren espacios de reunión o captación sin que puedan ser detectados. Un intento de cerrar toda "*puerta trasera*" para que solo las Agencias de inteligencia puedan hacer uso de ellas. [380]No obstante, *HRW* también indica que aunque se consiga cierto hermetismo en la seguridad de tales compañías de comunicaciones, las células terroristas seguirán desarrollando sus propios sistemas de desencriptación.

Por su parte, para otro observador como la *American Civil Liberties Union* (*ACLU*), las revelaciones de Snowden han puesto de manifiesto la hipocresía y la capitulación diplomática de los países que condenaron el espionaje de la *NSA* pero a la vez se negaron a ofrecer asilo político al ex analista.[381]Para la *ACLU* Snowden debe ser aplaudido y no vilipendiado, a la vez que se posiciona en favor de la concesión de inmunidad total frente a procesamientos judiciales y la posibilidad de que reanude su vida en los Estados Unidos.

*dos por defecto, y que ninguna de las empresas serían capaces de descifrar los datos almacenados en respuesta a las peticiones gubernamentales. Google, Microsoft, Yahoo, Facebook y otros han tomado ya medidas adicionales para asegurar correos electrónicos y mensajes*.
Véase Human Rights Watch: *Informe mundial 2015*, op. cit., p. 19.

378 Varios ataques cometidos en la noche del 13 de noviembre de 2015 en la capital francesa y su suburbio de Saint- Denis y perpetrados por atacantes suicidas que causaron 137 personas muertas y 415 heridas. La autoría de los ataques fue reivindicada por la organización yihadista Estado Islámico.

379 Human Rights Watch: *Informe mundial 2016*, p. 6,en: https://www.hrw.org/sites/default/files/world_report_download/wr2016_web.pdf

380 Una demostración de tal hecho han sido las peticiones del *FBI* a la compañía Apple para que ayudara a hackear el teléfono (*IPhone5*) de Syed Farook, el terrorista que mató a 14 personas a tiros en San Bernardino, California, el pasado 2 de diciembre.

381 ROMERO, D. Anthony: "Edward Snowden is a Patriot", December 17, 2013, *American Civil Liberties Union* (*ACLU*), en: https://www.aclu.org/blog/edward-snowden-patriot

## 7. Conclusiones.

Al comienzo de la investigación partíamos de una serie de hipótesis que vamos a tratar de refutar o rechazar en este espacio.

*1.-* Desde la redacción de la *National Security Act* de 1947, que dotaba de personalidad al aparato de inteligencia norteamericano, cada situación de crisis internacional, especialmente favorecidas por el clima de confrontación inaugurado con la Doctrina Truman, daría lugar a la correspondiente reestructuración organizativa de la comunidad de inteligencia, acompañada de nuevos departamentos, Agencias, normativas, directivas, etc; meros cambios cosméticos al servicio de los fines esenciales del Estado; iniciativas determinadas por la necesidad de aportar seguridad frente a un entorno internacional adverso, donde era preciso mantener a toda costa la posición de liderazgo mundial de Estados Unidos. Podría parecer que la función de inteligencia constituye una actividad, ajena a los intereses coyunturales de Gobierno, que responde ordenadamente a líneas de mando descendentes en defensa de los intereses generales del Estado. No obstante, el peso de la burocracia norteamericana es tan poderoso que obliga a un candidato a la presidencia como era Obama, quien defendía un discurso en contra de la vigilancia electrónica de ciudadanos norteamericanos, a llevar a cabo una acérrima defensa de los programas de vigilancia de la *NSA* una vez accedió a la presidencia de Estados Unidos en enero de 2009.

Tanto las Administraciones Bush como Obama han procurado la conformación de una estructura de inteligencia que se inauguró con la *USA PATRIOT ACT* en 2001 como mecanismo de respuesta rápida a los ataques del 11 de septiembre. En el camino hasta la actualidad, **las Administraciones han empleado la razón de Estado como herramienta para legitimar prácticas de dudosa legalidad** que vulneran principios democráticos de convivencia.

*2.-* **Lo que debieran ser instrumentos de control activo de las Agencias, han acabado erigiéndose en elementos serviles que no ponen objeciones a las prácticas, muchas veces invasivas, de las mismas.** Por ejemplo, el *Foreign Intelligence Surveillance Court* durante el período de actividad 1979-2013, tan sólo rechazó 12 órdenes de un total de 35.333. Lo que denota una política de concesión que apenas cuestiona la posible ilegalidad en las prácticas de las Agencias. Por su parte, la Ley *FISA* ha sido modificada en varias ocasiones desvirtuándose progresivamente su naturaleza de control.

La primera de estas reformas tuvo lugar el 16 de marzo de 2006, que otorgaba al Presidente mayor autoridad permitiendo que fuera el responsable de establecer una lista de grupos y organizaciones que están sujetas a la vigilancia electrónica autorizada bajo el *Terrorist Surveillance Program*. La siguiente reforma, de 18 de julio de 2006, posibilitó que el Presidente, a través del Fiscal General, pudiera autorizar la vigilancia electrónica sin una orden judicial para adquirir información de inteligencia extranjera. El 28 de julio de 2007, la inserción de la *Protect America Act* facilitó que se amparasen tanto al Director de Inteligencia Nacional como al Fiscal para autorizar, por períodos de hasta un año, la adquisición de información de inteligencia extranjera relativa a personas que se encuentran fuera de Estados Unidos. Finalmente el 20 de junio de 2008, la *FISA Amendments Act*, y más concretamente la Sección 702, recoge la posibilidad en beneficio del Gobierno, de utilizar una Ley que se oriente a la plena monitorización, tanto extranjera como nacional, para vigilar y someter la privacidad de ciudadanos estadounidenses.

Incluso la actual *USA FREEDOM ACT* hay que entenderla como una argucia política aprovechando la fecha de caducidad de la extinta *USA PATRIOT ACT*. Así, gracias a la *USA FREEDOM ACT,* el Gobierno no está obligado a dar explicaciones sobre el grueso de población investigada bajo la Sección 215 durante algo más de una década de la *USA PATRIOT ACT* o a informar sobre el número oficial de individuos investigados al amparo de la Sección 702 de la enmendada Ley *FISA*.

*3.-* Durante la Administración Obama la justificación de la existencia de los programas de vigilancia masiva desarrollados por la *NSA* ha sido la amenaza terrorista global. No obstante, el progreso tecnológico y la mejora de las capacidades de recogida y almacenamiento al alcance de la Agencia, **en efecto han posibilitado que sus programas de inteligencia ya no sólo tengan una aplicación directa sobre ciudadanos de todo el mundo con el pretexto de la lucha contra el terrorismo, sino también, que se hayan utilizado para adquirir ventajas comerciales,** como los casos de espionaje económico mediante escuchas e interceptación de emails de la compañía petrolera brasileña *Petrobras*, de reuniones económicas en Latinoamérica, de empresas eléctricas de Venezuela y México, así como espionaje efectuado a la petrolera *Gazprom* y la aerolínea *Aeroflot*, ambas rusas.

Del mismo modo, queda refutado que el sistema de vigilancia no conoce de aliados más que desde una perspectiva meramente estratégica, de intercambio de información. Así, países teóricamente aliados como Francia o Japón, fueron espiados con el único fin de conocer su consideración previa a la votación en el año 2010, cuando en el seno de la *ONU* se encontraban debatiendo sobre la necesidad, o no, de imponer nuevas sanciones al régimen iraní. **Es por tanto otra aplicación del sistema de vigilancia global de la NSA, la de adquisición de la ventaja política o de negociación.**

*4.-* Partiendo de la premisa anterior, si el Gobierno norteamericano legitima las prácticas invasivas de vigilancia de la *NSA* mediante la acción antiterrorista, podría parecer que Snowden ha expuesto a la comunidad de inteligencia no sólo al escarnio público sino al debilitamiento del sistema de seguridad que tanto se ha esforzado en construir frente a posibles células terroristas preparadas para el ataque. Sin embargo, la profundidad de actuación de los programas, obliga a entender que **Snowden no ha hecho sino denunciar las prácticas ilícitas de un sistema de seguridad no solo aplicable al ámbito terrorista sino también a la competitividad comercial así como intergubernamental.** Es por ello que **la presentación de Snowden como traidor resulta carente de sentido, cuando la estructura de vigilancia de por sí ya está justificada sobre una traición a la verdad, o en otras palabras, sobre la mentira antiterrorista.**

*5.-* Tras las revelaciones de los programas de vigilancia diversos países han rechazado la política de vigilancia invasiva del Gobierno norteamericano. Sin embargo, **se refuta que la hipocresía internacional ha sido la respuesta más extendida desde el panorama internacional ante el caso Snowden**. Esto ha sido así debido a la cooperación internacional de alguno de estos países con los programas de inteligencia que se esfuerzan en condenar, más aún cuando los programas siguen operativos. Este es el caso de Reino Unido mediante los programas *THIEVING MAGPIE* o *TEMPORA,* pero también, de servicios de inteligencia nacionales como el canadiense *Communications Security Establishment Canada* (*CSEC*) o la Agencia especializada en inteligencia electrónica de Australia, el *Defence Signals Directorate* (*DSD).* Incluso países como Alemania, que promovieron ante el Parlamento Europeo la condena sobre la vigilancia, mediante su servicio de inteligencia, el *Bundesnachrichtendienst* (*BND*), aportó registros de datos obtenidos dentro del país a cambio de tener acceso al programa *X-Keyscore*.

*6.-* La existencia de servicios de inteligencia en regímenes democráticos posibilita, en efecto, una paradoja política. Por un lado los servicios de inteligencia se establecen para proteger y garantizar la seguridad del Estado y el orden democrático. Por otro lado, en virtud de sus funciones, disponen del potencial suficiente para disolver la garantía democrática de los ciudadanos y alterar todo proceso democrático. **Resulta convincente tras la investigación, que los valores democráticos se vean afectados gravemente.** La consideración de la sociedad civil en su conjunto como un ente sospechoso sobre el que ceñir la política de vigilancia para anticipar amenazas futuras ayuda a socavar ya no sólo el ejercicio de la democracia entre los ciudadanos, sino también

la credibilidad y las relaciones de confianza entre países, quebrando así la política de la diplomacia.

Como se ha comentado, el comportamiento ejemplar no ha de llevar implícito el consentimiento para que las Agencias monitoricen y tengan acceso sin permiso a registros personales como historiales médicos o transacciones bancarias[382] pues puede haber individuos y grupos que no estén dispuestos a revelar sus secretos o ver expuesta una privacidad que no representa amenaza alguna para la seguridad del Estado. Por ejemplo, los periodistas que tratan de proteger a sus fuentes, los delatores, las personas que buscan ayuda en la red para aliviar sus tormentos psicológicos personales; adolescentes asustados que buscan consejo sobre la anticoncepción o el aborto, esposas de maridos distanciados por razones de violencia o abusos; solicitantes de asilo y refugiados disidentes; y un amplio etcétera.

382 Esto ha llevado consigo un importante coste económico directo en las corporaciones norteamericanas debido a la desconfianza generalizada que proporciona entre la población la idea de que las compañías suministren información confidencial a las Agencias de inteligencia. Empresas como *Microsoft*, *Yahoo!*, *Google*, *Facebook*, *Youtube*, *Skype*, *Apple* o *Dropbox*, se han visto comprometidas de cara a la opinión pública y aún a día de hoy no se conoce si estas corporaciones han trabajado facilitando la información a las Agencias o si estas últimas han extraído la información sin que se dieran cuenta.

## 8. BIBLIOGRAFÍA

Documentos oficiales de Estados Unidos.

Documentos audiovisuales.

Obras generales.

Obras específicas.

Observadores globales e Instituciones especializadas y Think Tanks.

OIG y ONG.

Publicaciones periódicas generales.

Publicaciones periódicas específicas.

### *DOCUMENTOS OFICIALES DE ESTADOS UNIDOS:*


BATES, D. John: *Memorandum Opinion*, United States Foreign Intelligence Surveillance Court, Washington DC, October 3, 2011.

BUSH, W. George: *President's Radio Address*, The Roosevelt Room, December 17, 2005.

Central Intelligence Agency (Office of Public Affairs), *A Consumer's Guide to Intelligence*, Washington, DC: Central Intelligence Agency, 1999.

CHENEY, Dick: *Defense Management. Report to the President*, Secretary of Defense, Washington, July 1989.

CLAPPER, R. James: *Office of the Director of National Intelligence*, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, June 8, 2013.

COLLINS. M. Susan: *Summary of Intelligence Reform and Terrorism Prevention Act of 2004*, United States Senate Committee on Governmental Affairs, December 2004.

Committee Church: *National Security Agency Surveillance Affecting Americans*, Book III, 1976.

Committee Amendment Proposed by Mr. Wyden (For himself and Mr. Udall of Colorado): *Report on The Implementation Of The FISA Amendments Act of 2008*, June 2012.

Declassified and approved for release by NSA, Top Secret, *BRITISH-U.S. Communication Intelligence Agreement, March 5, 1946*, Declassified on April 8, 2010.

Department of Defense Directive: *Directive nº 6. The National Security Agency and the Central Security Service*, December 23, 1971.

Executive order 12333: *United States Intelligence Activities,* U.S. President Ronald Reagan, December 4, 1981.

Executive order 12526: *President's Blue Ribbon Commission on Defense Management*, U.S. President Ronald Reagan, July 15, 1985.

Executive order 13284: *Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security*, U.S. President George W. Bush, January 23, 2003.

Executive order 13355: *Strengthened Management of the Intelligence Community*, U.S. President George

W. Bush, August 27, 2004.

Executive order 13470: *Further Amendments to Executive Order 12333, United States Intelligence Activities,* U.S. President George W. Bush, July 30, 2008.

National Security Council Intelligence: *Directive nº 9. Communications Intelligence,* 10 March 1950.

National Security Council Intelligence reform: *Directive nº 9. Communications Intelligence*, 29 December 1952.

Office of the Inspector General National Security Agency/Central Security Service*: Working Draft*, March 24, 2009.

Office of the Inspector General of the Department of Defense: *Requirements for the TRAILBLAZER and THINTHREAD Systems*, Deputy Inspector General for Intelligence, Audit Report, December 15, 2004.

Public Law 253-80th Congress: *The National Security Act of 1947*, July 26, 1947.

Public Law 216-81st Congress*: The National Security Act of 1947 as amended by Public Law 216*, approved August 10, 1949.

Public Law 511-95th Congress: *Foreign Intelligence Surveillance Act of 1978*, October 25, 1978.

Public Law 433-99th Congress: *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, October 1, 1986.

Public Law 56-107th Congress of the United States of America: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, (*USA PATRIOT ACT*) October 26, 2001.

Public Law 458-108th Congress: *Intelligence Reform and Terrorism Prevention Act of 2004*, December 17, 2004.

Public Law 55-110th Congress: *Protect America Act of 2007*, August 5, 2007. Public Law 261-110th Congress: *FISA Amendments Act of 2008*, July 10, 2008.

Public Law 23-114th Congress: *Uniting And Strengthening America By FulFilling Rights And Ensuring Effective Discipline Over Monitoring Act of 2015*, (*USA FREEDOM ACT*) June 2, 2015.

Report Prepared by the Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Office of the Director of National Intelligence*: Unclassified Report on the President´s Surveillance Program*, Report nº 2009-0013-AS, July 10, 2009.

Select Committee to Study Governmental Operations: *Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, United States: Congress, Library of Congress, Washington, April 29, 1976.

Senate and House of Representatives of the United States of America in Congress assembled:

*Communications Act of 1934,* June 1934.

Special Source Operations: *FAIRVIEW and STORMBREW: 'Live' - On the Net*, Dynamic page – Highest possible classification is TOP SECRET, November 19, 2003.

*The Constitution of United States*, September 17, 1787.

The National Commission on Terrorist Attacks Upon the United States: *The 9/11 Comission Report*, 2004.

TRUMAN, S. Harry: *Memorandum from President Harry S. Truman to the Secretary of State*, the Secretary of Defense, Subject: Communications Intelligence Activities, 24 October 1952.

United States Code (*USC*) Title 10: Armed Forces, §§ 801–946: *The Uniform Code of Military Justice*

(*UCMJ*), May 31, 1951.

United States Foreign Intelligence Surveillance Court*: Full order Roger Vinson*, Washington D.C., July 19, 2013.

United States Government: *Executive Order 12333*, as Amended by Executive Orders *13284* (2003),

*13355* (2004) and *13470* (2008), December 4, 1981.

WYDEN, Ron: *Prepared Remarks of Senator Ron Wyden on a Bill to Extend the FISA Amendments Act of 2008*.

WYDEN, Ron & UDALL, Mark: *Letter to General Keith Alexander*, United States Senate, Washington DC, October 10, 2012.

107th Congress-2d Session, The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence: *Report of the joint inquiry into the terrorist attacks of September 11, 2001*, December 2002.

109th Congress-2d Session, Dewine, Mark, & Graham, Lindsey, & Hagel, Chuck, & Snowe, Olympia:

*Terrorist Surveillance Act of 2006*, 2006.

114th Congress: *USA FREEDOM ACT of 2015*, June 2, 2015.

## DOCUMENTOS AUDIOVISUALES:

GREENWALD, Glenn: *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things*, Interview Hotel Mira Hong Kong, June 6, 2013, *The Guardian*, en: https://www.youtube.com/watch?v=5yB3n9fu-rM

POITRAS, Laura, Documental: *Citizenfour*, Praxis Films, Estados Unidos, 114 min, 2014.

*President Obama's Full NSA Speech*, January 17, 2014, en: https://www.youtube.com/watch?-v=p4MKm2uFqVQ

Senator Ron Wyden questions Director of National Intelligence, James Clapper, *Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?*, March 2013, *The Guardian*, en: http://www.theguardian.com/world/video/2013/jun/07/privacy-wyden-clapper-nsa-video

## OBRAS GENERALES:

BERKOWITZ, Bruce: *The National Reconnaissance Office at 50 years: A brief history*, Center for the Study of National Reconnaissance, National Reconnaissance Office, Chantilly, Virginia, Ed: Government Printing Office, 2011.

BIGELOW, Bill, & McGAULEY, Sylvia, & McKENNA, Tom, & HYUNG, Nam, & TREICK

O'NEILL, Julie: *The Most Dangerous Man in America: Daniel Ellsberg and the Pentagon Papers*, Teaching guide, Zinn Education Project, Washington DC, 2010.

CALDUCH, Rafael: *Dinámica de la Sociedad Internacional*, Colección de información y comunicación, Madrid, Ed: Centro de Estudios Ramón Areces, 1993.

CALDUCH, Rafael: *Métodos y técnicas de investigación en Relaciones Internacionales*, Ed: Universidad Complutense de Madrid, 2003.

CHURCHILL, W. & VANDER WALL, J: *The COINTELPRO Papers. Documents from the FBI's*

*Secret Wars against Domestic Dissent*, Boston, Ed: South End Press, 1990.

DAHL, A. Robert: *La Democracia*, Ed: Ariel Quintaesencia, ed. 2012. ESTULIN, Daniel: *Desmontando WikiLeaks*, Ed: Bronce, 2011.

JOHNSON, R. Thomas: *American Cryptology during the Cold War; 1945-1989*, Book III, Series VI, Volume V, National Security Agency & Central Security Service, 2007.

PRIEST, Dana & ARKIN, William: *Top Secret America: The Rise of the New American Security State*, Ed: Little, Brown and Company, 2011.

RAMONET, Ignacio: *El imperio de la vigilancia*, Ed: Clave Intelectual, 2016.

RECORD, Jeffrey: *Bounding the Global War On Terrorism,* Strategic Studies Institute, Ed: Lulu, 2003.

SEGOVIANO, Soledad: *La acción encubierta como instrumento de la política exterior norteamericana*. (Tesis doctoral). Departamento de Derecho Internacional Público y Relaciones Internacionales (Estudios Internacionales), Facultad de Ciencias de la Información, Universidad Complutense de Madrid, 1997.

## OBRAS ESPECÍFICAS:

BAMFORD, James: *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, Ed: Anchor Books, 2002.

BAMFORD, James: *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, Boston, Ed: Houghton Mifflin Harcourt, 1982.

BAMFORD, James: *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America,* New York, Ed: Doubleday, 2009.

BURNS, L. Thomas: *The Origins of the National Security Agency 1940-52,* Center for Cryptologic History, U.S. National Security Agency (*NSA*), Chapter IV: "Creation of the Armed Forces Security Agency", Series V: Volume I, 1990.

CAMBONE, A. Stephen: *A New Structure for National Security Policy Planning*, Ed: Center for Strategic & International Studies, 1998.

GREENWALD, Glenn: *Snowden: Sin un lugar donde esconderse*, Ediciones B, 2014.

JOHNSON, K. Loch: *A Season of Inquiry: The Senate Intelligence Investigation*, Lexington, Ed: University Press of Kentucky, 1985.

KENT, Sherman: *Strategic Intelligence for American World Policy*, Ed. Princeton, NJ: Princeton University Press, 1966.

LEFEBURE, Antoine: *El caso Snowden: Así espía Estados Unidos al mundo*, Ed: Clave Intelectual, 2014.

## OBSERVADORES GLOBALES E INFORMES DE INSTITUCIONES ESPECIALIZADAS Y THINK TANKS:

BAZAN, B. Elizabeth: *Electronic Surveillance Modernization Act*, as Passed by the House of Representatives, CRS Report for Congress, Legislative Attorney American Law Division, January 2007.

BraveNew Foundation: *War on whistleblowers*. Free press and the National Security State, discussion and resource guide.

Canadian Journalists for Free Expression (*CJFE*), Snowden Archive, *FAIRVIEW: CLIFFSIDE Site - Collection Resumes After 5 Months*, August 23, 2011.

Center For Democracy and Technology (*CDT*), *Comparison of 2014 and 2015 versions of the USA FREEDOM ACT,* April 28, 2015.

CHARRETT, Catherine: *A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security*, International Catalan Institute for Peace (ICIP), Working Papers, December 2009.

COX, S. James: "Canada and the Five Eyes Intelligence Community", *Strategic Studies Working Group Papers*, Canadian International Council, December 2012.

DAVIES, Simon: *A Crisis of Accountability. A global analysis of the impact of the Snowden revelations*, The Privacy Surgeon, published in association with Institute for Information Law and Law, Science, Technology & Society Studies, June 2004.

Geneva Centre for Democratic Control of Armed Forces: *Intelligence Services and Democracy*, Working paper series, nº 13, Switzerland, April 2002.

HEATH, J. Laura: *An analysis of the systemic security weaknesses of the U.S. Navy fleet broadcasting system, 1967-1974, as exploited by CWO John Walker*, M.S., Georgia Institute of Technology, Fort Leavenworth, Kansas, 2001.

KEHL, Danielle & BANKSTON, Kevin & GREENE, Robyn & MORGUS, Robert: *Surveillance Costs: The NSA´s Impact on the Economy, Internet Freedom & Cibersecurity*, New America´s Open Technology Institute, Policy Paper, July 2014.

LIU, C. Edward, & NOLAN, Andrew, & THOMPSON, M. Richard: *Overview of Constitutional Challenges to NSA Collection Activities*, Congressional Research Service, CRS Report, May 21, 2015.

METZ, Steven & KIEVIT, James: *Strategy and the Revolution in Military Affairs: from theory to policy*, Strategic Studies Institute, US Army War College, June 27, 1995.

NEMFAKOS, Charles & BLICKSTEIN, Irv & McCARTHY, Aine Seitz & SOLINGER, M. Jerry: *The Perfect Storm. The Goldwater-Nichols Act and its effect on Navy acquisition*, National Defense Research Institute, Occasional paper, RAND corporation, 2010.

NICHOL, Jim: *Russian political, economic, and security issues and U.S. interests*, Congressional Research Service, CRS Report, March 31, 2014.

ROLLINS, John & HENNING, C. Anna: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, Congressional Research Service, CRS Report, March 10, 2009.

Sandvine: Intelligent Broadcast Networks, *Global Internet Phenomena Report*, 1H 2014, Canada, en: https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/2h-2014-global-internet- phenomena-report.pdf

VAN CLEAVE, Michelle: *Myth, Paradox and the obligations of leadership: Edward Snowden, Bradley Manning and the Next Leak*, Center for Security Policy, Occasional Paper Series, Washington DC, September 13, 2013.

WELT, Cory: *What the Snowden affair says about U.S.-Russian relations*, Center for American Progress, July 17 2013.

WikiLeaks. *Afghanistan war logs*, July 25, 2010, en: https://wikileaks.org/afg/

WikiLeaks: *Baghdad Airstrike/Collateral Murder*, April 5, 2010, en: https://www.youtube.com/watch?v=Ojw5MnsqkJQ

WikiLeaks. *Collateral Murder,* 5 Apr 2010, en: https://wikileaks.org/wiki/Collateral_Murder,_5_Apr_2010

WikiLeaks. Global Intelligence Files leak, February 27, 2012, en: https://wikileaks.org/gifiles/

WikiLeaks. *Iraq War Logs*, October 22, 2010, en: https://wikileaks.org/irq/

WikiLeaks. *¿Qué es WikiLeaks.org?* en: https://wikileaks.org/wiki/Wikileaks/es

WikiLeaks. *US Iraq Rules of Engagement leaked*, February 4, 2008, en: https://wikileaks.org/wiki/US_Iraq_Rules_of_Engagement_leaked

## OIG y ONG:

American Civil Liberties Union (*ACLU*): *ACLU comment on Bradley Manning sentence*, August 21, 2013.

Asamblea General de Naciones Unidas: *Declaración Universal de los Derechos Humanos,* Adoptada y proclamada por la Resolución de la Asamblea General 217, del 10 de Diciembre de 1948.

Asamblea General de Naciones Unidas: *Pacto Internacional de Derechos Civiles y Políticos*, Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su Resolución 2200, de 16 de Diciembre de 1966.

British Columbia Civil Liberties Association, *Spying in Canada: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying on Canadians*, October 22, 2013.

Consejo de Derechos Humanos: *El derecho a la privacidad en la era digital*, 28º período de sesiones A/HRC/28/L.27, Naciones Unidas, Asamblea General, Marzo 24, 2015.

European Parliament: *Report on the existence of a global system for the interception of private and commercial communications* (*ECHELON* interception system), 11 July 2001.

Human Rights Council: *The right to privacy in the digital age*, Report of the Office of the UnitedNations High Commissioner for Human Rights, Twenty-seventh session. A/HRC/27/37, June 30, 2014.

Human Rights Watch: *Informe mundial 2014*. Human Rights Watch: *Informe mundial 2015*. Human Rights Watch: *Informe mundial 2016*.

Naciones Unidas, Asamblea General: *Resolución aprobada por la Asamblea General* el 18 de Diciembre de 2014 [sobre la base del informe de la Tercera Comisión (A/69/488/Add.2 y Corr.1)], Sexagésimo noveno período de sesiones A/RES/69/166, Febrero 10, 2015.

Parlamento Europeo. Comisión de Libertades Civiles, Justicia y Asuntos de Interior: Documento de sesión. *Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior*, (2013/2188(INI)), A7-0139/2014, Febrero 21, 2014.

Regulation of the European Parliament and of the Council: *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), Brussels, 25 January 2012.

ROMERO, D. Anthony: "Edward Snowden is a Patriot", December 17, 2013, *American Civil Liberties Union* (ACLU), en: https://www.aclu.org/blog/edward-snowden-patriot

United Nations, General Assembly: *Resolution adopted by the General Assembly* on 18 December 2013 [on the report of the Third Commi-

ttee (A/68/456/Add.2)], Sixty-eighth session A/RES/68/167, January 21, 2014.

## PUBLICACIONES PERIÓDICAS GENERALES:

ACKERMAN, Spencer & BALL, James: "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", February 27, 2014, *The Guardian*.

ANTONIO, O. Gabriel: "El aporte de la Escuela de Copenhague a los estudios de seguridad", *Revista Fuerzas Armadas y Sociedad*, nº 1, 2000.

BALL, James, & BORGER, Julian, & GREENWALD, Glenn: "Revealed: how US and UK spy agencies defeat internet privacy and security", September 6, 2013, *The Guardian*.

BAMFORD, James: "Watch the neighbor", March 11, 2016, *Foreign Policy*.

BOWCOTT, Owen: "GCHQ surveillance hearing to begin", July 14, 2014, *The Guardian*.

BRAKE, Benjamin: "The Bug trade: Regulating the Rise of Post-Snowden Spyware", April 22, 2015,

Foreign Affairs.

BRISSENDEN, Michael: "Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked

Edward Snowden documents reveal", December 04, 2014, *ABC News*.

BUZAN, Barry: "New Patterns of Global Security in the Twenty-First Century", *International Affairs*, Vol. 67, nº 3, July 1991.

BYMAN, Daniel & WITTES, Benjamin: "Reforming the NSA: How to spy after Snowden", May/June

2014 Issue, *Foreign Affairs*.

CAMPBELL, Duncan: "They've got it taped", August 12, 1988, *The New Statesman*.

CAULEY, Leslie. "NSA has massive database of Americans' phone calls", May 11, 2006, *USA Today*. CAULEY, Leslie., DIAMOND, John., DRINKARD, Jim., EISLER, Peter., FRANK, Thomas., JOHSON,

Kevin., et al. "Lawmakers: NSA database incomplete ", June 30, 2006, *USA Today*.

CLIVE, P. Keith: "NSA´s Central Security Service", *U.S. Military Academy´s Cryptologia*, 2002.

COMA, Manuel: "Fallos de inteligencia y responsabilidades gubernamentales", *Fundación para el Análisis y los Estudios Sociales (FAES)*, Cuadernos de pensamiento político nº 4, Octubre-Diciembre 2004.

DAVIS, C. Norman: "An Information-Based Revolution in Military Affairs", *Strategic Review*, U.S. Strategic Institute, Vol. 24, nº 1, Winter 1996.

DÍAZ MATEY, Gustavo: "La Comunidad de Inteligencia estadounidense tras las elecciones de noviembre de 2008: retos y oportunidades de la administración Obama", *Real Instituto Elcano*, Documento de Trabajo nº 6, 5 Febrero, 2009.

DÍAZ MATEY, Gustavo: "The U.S. Intelligence Reform and the National Intelligence Strategy of

October 2005", *Revista UNISCI*, nº 10, Enero 2006.

DYER, Geoff: "US Republicans face NSA dilemma", US Politics & Policy, November 19, 2014,

*Financial Times*.

ENSOR, David: "How Washington can win the Information War", December 14, 2015, *Foreign Policy*.

Editorial board: "President Obama's Dragnet", June 6, 2013, *The New York Times*.

GREENWALD, Glenn: "Obama's NSA 'reforms' are little more than a PR attempt to mollify the public",

January 17, 2014, *The Guardian*.

GREENWALD, Glenn: "XKeyscore: NSA tool collects nearly everything a user does on the internet",

July 31, 2013, *The Guardian*.

GREENWALD, Glenn & ACKERMAN, Spencer: "How the NSA is still harvesting your online data",

June 27, 2013, *The Guardian*.

GREENWALD, Glenn, & KAZ, Roberto & CASADO, José: "US spied on millions of emails and Brazilian bonds", July 7, 2013, *O Globo*.

GREENWALD, Glenn & MACASKILL, Ewen: "Boundless Informant: the NSA's secret tool to track global surveillance data". June 11, 2013, *The Guardian.*

GREENWALD, Glenn, & MACASKILL, Ewen: "NSA Prism program taps in to user data of Apple, Google and others", June 7, 2013, *The Guardian*.

GREENWALD, Glenn & MACASKILL, Ewen & POITRAS, Laura & ACKERMAN, Spencer & RUSHE, Dominic: "Microsoft handed the NSA access to encrypted messages", July 12, 2013, *The Guardian*.

GROLL, Elias: "When the NSA is a hacker´s best friend", December 23, 2015, *Foreign Policy*.

HOPKINS, Nick: "Surveillance, democracy, transparency – a global view", October 10, 2013, *The Guardian*.

KONCZAL, Mike: "Is a democratic surveillance state possible?", June 8, 2013, *The Washington Post*.

LICHTBLAU, Eric. "In Secret, Court Vastly Broadens Powers of N.S.A", July 6, 2013, *The New York Times*.

LOCHER III, R. James: "Has it worked? The Goldwater-Nichols Reorganization Act", *Naval War College Review*, Vol. LIV, nº 4, Autumn 2001.

LORENTE, Adolfo & CHAMORRO, Enrique & PIELLA, Guillem: "Vigilados por defecto", *Instituto Español de Estudios Estratégicos* (*IEEEs*), nº 34, 4 Abril, 2014.

MACASKILL, Ewen, & BORGER, Julian, & HOPKINS, Nick, & DAVIES, Nick, & BALL, James: "GCHQ taps fibre-optic cables for secret access to world's communications", June 21, 2013, *The Guardian*.

MAYER, Jane: "The Secret Sharer", May 23, 2011, *The New Yorker*.

MERCER, Jonathan: "Anarchy and Identity", *International Organization*, Vol. 49, nº 2, 1995.

NAUGHTON, John: "The NSA has us snared in its trap – and there's no way out", June 15, 2013, *The Observer*.

POZO, S. Pilar: "Externalización de funciones de inteligencia: oportunidades y riesgos a la luz de la experiencia estadounidense", *Inteligencia y seguridad,* nº 6, 2009.

ROWLEY, Coleen: "Coleen Rowley's Memo to FBI Director Robert Mueller An edited version of the agent's", Washington D.C., May 21, 2002, *TIME Online Edition.*

SÁINZ, José Antonio: "Inteligencia táctica". *Revista UNISCI*, nº 28, Enero 2012.

SÁNCHEZ, H. Carlos: "Analogías de la historia I: Julian Assange y Wikileaks vs Daniel Ellsberg y los

Pentagon Papers", *Revista Crítica de Ciencias Sociales y Jurídicas*, *UCM*, nº 31, Marzo 2011.

SAVAGE, Charlie & WYATT, Edward. "U.S. Is Secretly Collecting Records of Verizon Calls", June 5,

2013, *The New York Times*.

SEYMOUR, Richard. "Obama's Verizon phone records collection carries on Bush's work", June 6, 2013,

*The Guardian*.

TARIF, Mathilde: "Legitimizing the use of covert action in the eyes of the American people", July 21,

2015, *Hestia Expertise*.

WHALEN, Jeanne & CRAWFORD, David: "How WikiLeaks keeps its funding secret", August 23, 2010,

*The Wall Street Journal*.

## PUBLICACIONES PERIÓDICAS ESPECÍFICAS:

BAMFORD, James: "The NSA and Me", October 2, 2014, *The Intercept*.

BUMP, Philip: "The UK Tempora Program Captures Vast Amounts of Data and Shares with NSA", June

21, 2013, *The Wire*.

FROOMKIN, Dan: "After Two Years, White House Finally Responds to Snowden Pardon Petition – With a "No", July 28, 2015, *The Intercept*.

FROOMKIN, Dan: "U.N. Report Calls on Governments to Protect Whistleblowers Like Snowden, Not Prosecute Them", October 23, 2015, *The Intercept*.

GREENWALD, Glenn: "Exploiting Emotions About Paris to Blame Snowden, Distract from Actual Culprits Who Empowered ISIS", November 15, 2015, *The Intercept*.

HARRIS, Shane: "CIA's Ex-No. 2 Says ISIS 'Learned From Snowden", May 6, 2015, *NewAmerica.org*. KEHL, Danielle: "The Cost of NSA Surveillance", October 1, 2014, *NewAmerica.org*.

McLAUGHLIN, Jenna: "European Parliament Says Snowden Should Be Welcomed in Europe", October 29, 2015, *The Intercept*.

McLAUGHLIN, Jenna: "Senate Kicks Off Debate Over Reauthorizing Controversial NSA Programs", May 10, 2016, *The Intercept*.

McLAUGHLIN, Jenna: "U.S. Mass Surveillance Has No Record of Thwarting Large Terror Attacks, Regardless of Snowden Leaks", November 17, 2015, *The Intercept*.

MORGUS, Robert & KEHL, Danielle: "The Wrong Way to Respond to the Snowden Revelations", December 19, 2014, *NewAmerica.org*.

SCHWARZ, Jon: "Snowden Effect" in Action: NSA Authority to Collect Bulk Phone Metadata Expires", November 29, 2015, *The Intercept*.

# 9. ANEXO APÉNDICES

APÉNDICE **(A)**:

*Fragmentos de la National Security Act*. [1947]
APÉNDICE **(B)**:

National Security Council Intelligence: *Directive nº 9. Communications Intelligence.* [1950]
APÉNDICE **(C)**:

*Fragmentos de la Foreign Intelligence Surveillance Act*. [1978] APÉNDICE **(D)**:

*Fragmentos de la USA PATRIOT ACT*. [2001]
APÉNDICE **(E)**:

*Fragmentos de la FISA Amendments Act.* [2008].

APÉNDICE **(F)**:

*Orden del Juez Roger Vinson a la compañía Verizon. [2013]*

APÉNDICE **(G)**:

Fragmentos de la USA FREEDOM ACT. [2015]

## 9.1. APÉNDICE A:

**Fragmentos de la National Security Act [1947]**

# The National Security Act of 1947 – July 26, 1947

Public Law 253, 80th Congress; Chapter 343, 1st Session; S. 758.

## AN ACT

To promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with national security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

## SHORT TITLE

That this Act may be cited as the "National Security Act of 1947".

## TABLE OF CONTENTS

Sec.2. Declaration of policy

### TITLE I—COORDINATION FOR NATIONAL SECURITY

Sec. 101. National Security Council.
Sec. 102. Central Intelligence Agency.
Sec. 103. National Security Resources Board.

### TITLE II—THE NATIONAL MILITARY ESTABLISHMENT

Sec. 201. National Military Establishment.
Sec. 202. Secretary of Defense.
Sec. 203. Military Assistants to the Secretary.
Sec. 204. Civilian personnel.
Sec. 205. Department of the Army.
Sec. 206. Department of the Navy.
Sec. 207. Department of the Air Force.
Sec. 208. United States Air Force.
Sec. 209. Effective date of transfers.
Sec. 210. War Council.
Sec. 211. Joint Chiefs of Staff.
Sec. 212. Joint Staff.
Sec. 213. Munitions Board.
Sec. 214. Research and Development Board.

### TITLE III—MISCELLANEOUS

Sec. 301. Establishment of Compensation of Secretaries.
Sec. 302. Under Secretaries and Assistant Secretaries.
Sec. 303. Advisory committees and personnel.
Sec. 304. Status of transferred civilian personnel.

Sec. 305. Saving provisions.
Sec. 306. Transfer of funds.
Sec. 307. Authorization for appropriations.
Sec. 308. Definitions.
Sec. 309. Separability.
Sec. 310. Effective date.
Sec. 311. Succession to the Presidency.

## DECLARATION OF POLICY

Sec. 2. In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States, to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide three military departments for the operation and administration of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force, with their assigned combat and service components; to provide for their authoritative coordination and unified direction under civilian control but not to merge them; to provide for the effective strategic direction of the armed forces and for their operation under unified control and for their integration into an efficient team of land, naval, and air forces.

## TITLE I—COORDINATION FOR NATIONAL SECURITY

### National Security Council

Sec. 101.

(a) There is hereby established a council to be known as the National Security Council (hereinafter in this section referred to as the "Council").

The President of the United States shall preside over meetings of the Council: PROVIDED, That in his absence he may designate a member of the council to preside in his place.

The function of the Council shall be to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.

The Council shall be composed of the President; the Secretary of State, the Secretary of Defense, appointed under section 202; the Secretary of the Army, referred to in section 205; the Secretary of the Navy; the Secretary of the Air Force, appointed under section 207; the chairman of the National Security Resources Board, appointed under section 103; and such of the following named officers as the President may designate from time to time: The Secretaries of the executive departments, the Chairman of the Munitions Board appointed under section 213, and the chairman of the Research and Development Board appointed under section 214; but no such additional member shall be designated until the advice and consent of the Senate has been given to his appointment to the office the holding of which authorizes his designation as a member of the Council.

(b) In addition to performing such other functions as the President may direct, for the purpose of more effectively coordinating the policies and functions of the departments

and agencies of the Government relating to the national security, it shall, subject to the direction of the President, be the duty of the council—

(1) to assess and appraise the objectives, commitments, and risks of the United States in relation to our actual and potential military power, in the interest of national security; for the purpose of making recommendations to the President in connection therewith; and

(2) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith.

(c) The Council shall have a staff to be headed by a civilian executive secretary who shall be appointed by the President, and who shall receive compensation at the rate of $10,000 a year. The executive secretary, subject to the direction of the Council, is hereby authorized, subject to the civil service laws and the Classification Act of 1923, as amended, to appoint and fix the compensation of such personnel as may be necessary to perform such duties as may be prescribed by the council in connection with the performance of its functions.

(d) The Council shall, from time to time, make such recommendations, and such other reports to the President as it deems appropriate or as the President may require.

**Central Intelligence Agency**

Sec. 102.

(a) There is hereby established under the National Security Council a Central Intelligence Agency with a Director of Central Intelligence, who shall be the head thereof. The Director shall be appointed by the President, by and with the advice and consent of the Senate, from among the commissioned officers of the armed services or from among individuals in civilian life. The Director shall receive compensation at the rate of $14,000 a year.

(b)

(1) If a commissioned officer of the armed services is appointed as Director then—

(A) in the performance of his duties as Director, he shall be subject to no supervision, control, restriction, or prohibition (military or otherwise) other than would be operative with respect to him if he were a civilian in no way connected with the Department of the Army, the Department of the Navy, the Department of the Air Force, or the armed services or any component thereof; and

(B) he shall not possess or exercise any supervision, control, powers, or functions (other than such as he possesses, or is authorized or directed to exercise, as Director) with respect to the armed services or any component thereof, the Department of the Army, the Department of the Navy, or the Department of the Air Force, or any branch, bureau, unit or division

thereof, or with respect to any of the personnel (military or civilian) of any of the foregoing.

(2) Except as provided in paragraph (1), the appointment to the office of Director of a commissioned officer of the armed services, and his acceptance of and service in such office, shall in no way affect any status, office, rank, or grade he may occupy or hold in the armed services, or any emolument, perquisite, right, privilege, or benefit incident to or arising out of any such status, office, rank, or grade. Any such commissioned officer shall, while service in the office of Director, receive the military pay and allowances (active or retired, as the case may be) payable to a commissioned officer of his grade and length of service and shall be paid, from any funds available to defray the expenses of the Agency, annual compensation at a rate equal to the amount by which $14,000 exceeds the amount of his annual military pay and allowances.

(c) Notwithstanding the provisions of section 6 of the Act of August 24, 1912 (37 Stat. 555), or the provisions of any other law, the director of Central Intelligence may, in his discretion, terminate the employment of any officer or employee of the Agency whenever he shall deem such termination necessary or advisable in the interests of the United States, but such termination shall not affect the right of such officer or employee to seek or accept employment in any other department or agency of the Government if declared eligible for such employment by the United States Civil Service Commission.

(d) For the purpose of coordinating the intelligence activities of the several Government departments and agencies in the interest of national security, it shall be the duty of the Agency, under the direction of the National Security Council—

(1) to advise the National Security Council in matters concerning such intelligence activities of the Government departments and agencies as relate to national security;

(2) to make recommendations to the National Security Council for the coordination of such intelligence activities of the departments and agencies of the Government as relate to the national security;

(3) to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence within the Government using where appropriate existing agencies and facilities: PROVIDED, That the Agency shall have no police, subpoena, law-enforcement powers, or internal-security functions: PROVIDED FURTHER, That the departments and other agencies of the Government shall continue to collect, evaluate, correlate, and disseminate departmental intelligence: AND PROVIDED FURTHER, That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure;

(4) to perform, for the benefit of the existing intelligence agencies, such additional services of common concern as the National Security council determines can be more efficiently accomplished centrally;

(5) to perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct.

(3) policies for unifying, in time of war, the activities of Federal agencies and departments engaged in or concerned with production, procurement, distribution, or transportation of military or civilian suppose, materials, and products;

(4) the relationship between potential supplies of, and potential requirements for, manpower, resources, and productive facilities in time of war;

(5) policies for establishing adequate reserves of strategic and critical material, and for the conservation of these reserves;

(6) the strategic relocation of industries, services, government, and economic activities, the continuous operation of which is essential to the Nation's security.

(d) In performing its functions, the Board shall utilize to the maximum extent the facilities and resources of the departments and agencies of the Government.

## TITLE II—THE NATIONAL MILITARY ESTABLISHMENT

### Establishment of the National Military Establishment

Sec. 201.

(a) There is hereby established the National Military Establishment, and the Secretary of Defense shall be the head thereof.

(b) The National Military Establishment shall consist of the Department of the Army, the Department of the Navy, and the Department of the Air Force, together with all other agencies created under title II of this Act.

### Secretary of Defense

Sec. 202.

(a) There shall be a Secretary of Defense, who shall be appointed from civilian life by the President, by and with the advice and consent of the Senate: PROVIDED, That a person who has within ten years been on active duty as a commissioned officer in a Regular component of the armed services shall not be eligible for appointment as Secretary of Defense. The Secretary of Defense shall be the principal assistant to the President in all matters relating to the national security. Under the direction of the President and subject to the provisions of the Act he shall perform the following duties:

(1) Establish general policies and programs for the national Military Establishment and for all of the departments and agencies therein:

(2) Exercise general direction, authority, and control over such departments and agencies;

(3) Take appropriate steps to eliminate unnecessary duplication or overlapping in the fields of procurement, supply, transportation, storage, health, and research;

(4) Supervise and coordinate the preparation of the budget estimates of the departments and agencies comprising the National Military Establishment; formulate and determine the budget estimates for submittal to the Bureau of the Budget; and supervise the budget programs of such departments and agencies

## 9.2. APÉNDICE B:

National Security Council Intelligence:

**Directive nº 9. Communications Intelligence [1950]**

C O P Y

UNCLASSIFIED

NSCID 9
Revised
March 10, 1950

NATIONAL SECURITY COUNCIL INTELLIGENCE DIRECTIVE NO. 9

COMMUNICATIONS INTELLIGENCE

Pursuant to the provisions of Section 101 and Section 102 of the National Security Act of 1947, as amended, the National Security Council hereby authorizes and directs that:

1. There is hereby established under the National Security Council the United States Communications Intelligence Board (hereinafter referred to as the "Board") to effect the authoritative coordination of Communications Intelligence activities of the Government and to advise the Director of Central Intelligence in those matters in the field of Communications Intelligence for which he is responsible.

2. The Board will be composed of not to exceed two members from each of the following departments or agencies: The Departments of State, the Army, the Navy, and the Air Force, and the Central Intelligence Agency, and the Federal Bureau of Investigation. Only those departments or agencies designated by the President are authorized to engage in Communications Intelligence activities.

3. The Board members will be vested with authority to represent their respective departments or agencies in the field of Communications Intelligence and each member department or agency will be represented at each meeting by at least one member, or alternate, with the necessary powers to act.

4. Decisions of the Board will be based on the principle of unanimity, which shall be a prerequisite for matters within the purview of the Board, except that the Chairman shall be elected by majority vote. When decision cannot be reached, the Board will promptly refer the matter for resolution to the National Security Council; provided that, when unanimity is not obtained among the military department heads of the Department of Defense, the Board shall present the problem to the Secretary of Defense before presenting it to the National Security Council.

5. Decisions and policies promulgated by the Board within the scope of its jurisdiction shall be applicable to all departments and agencies represented on or subordinate to the National Security Council and any others designated by the President, and shall be implemented by those departments and agencies of which action is required.



1 par 5

NSCID 9
Revised
March 10, 1950

Declassified/Downgraded
By the National Security Council
under provisions of E.O. 10501
by

UNCLASSIFIED

UNCLASSIFIED

6. The special nature of Communications Intelligence activities requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to Communications Intelligence activities, unless specifically so stated and issued by competent departmental or agency authority represented on the Board.

7. The Board shall act for the National Security Council to insure proper and full implementation of Council directives by issuing such supplementary directives as may be required. Such implementing directives in which the Board concurs unanimously shall be issued to and implemented by the member departments and agencies. When disagreement arises in the Board upon such directive, the proposed directive, together with statement of non-concurrence, shall be forwarded to the National Security Council for decision as provided in paragraph 4.

8. Other National Security Council Intelligence Directives to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to Communications Intelligence activities under the authority of paragraph 6 above, unless the National Security Council has made its directive specifically applicable to Communications Intelligence.

9. The Board will perform such functions as may be required to accomplish its objective set forth in paragraph 1 above, and in the exercise of responsibilities and authority delegated to it by the National Security Council in this directive.

10. The Board shall leave the internal administration and operation of Communications Intelligence activities to the member departments or agencies.

11. All currently effective decisions, policies, and operating arrangements of the Board and its predecessors, the Army-Navy Communications Intelligence Board, and the State-Army-Navy Communications Intelligence Board, as previously constituted, which are not in conflict with this directive, will remain in full force and effect unless changed by subsequent decisions of the Board.

12. Definitions. For purposes of this directive the following definitions apply:

a. "Foreign communications" include all telecommunications and related materials (except Foreign Press and Propaganda Broadcasts) of the government



9
ed
n 10, 1950

UNCLASSIFIED

and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor; they shall include all other telecommunications and related material of, to, and from a foreign country which may contain information of military, political, scientific or economic value.

b. "Communications Intelligence" is intelligence produced by the study of foreign communications. Intelligence based in whole or in part on Communications Intelligence sources shall be considered Communications Intelligence as pertains to the authority and responsibility of the United States Communications Intelligence Board.

c. "Communications Intelligence Activities" comprise all processes involved in the collection, for intelligence purposes, of foreign communications, the production of information from such communications, the dissemination of that information, and the control of the protection of that information and the security of its sources.



USCIB 9
ised
h 10, 1950

## 9.3. APÉNDICE C:

Fragmentos de la Foreign Intelligence Surveillance Act [1978]

# FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 [1]

[Public Law 95–511; 92 Stat. 1783; approved October 25, 1978]

[As Amended Through P.L. 114–23, Enacted June 2, 2015]

AN ACT To authorize electronic surveillance to obtain foreign intelligence information.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,* That [50 U.S.C. 1801 nt] this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

Sec. 101. Definitions.
Sec. 102. Authorization for electronic surveillance for foreign intelligence purposes.
Sec. 103. Designation of judges.
Sec. 104. Application for an order.
Sec. 105. Issuance of an order.
Sec. 106. Use of information.
Sec. 107. Report of electronic surveillance.
Sec. 108. Congressional oversight.
Sec. 109. Penalties.
Sec. 110. Civil liability.
Sec. 111. Authorization during time of war.
Sec. 112. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.

TITLE II—CONFORMING AMENDMENTS

Sec. 201. Amendments to chapter 119 of title 18, United States Code.

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

Sec. 301. Definitions.
Sec. 302. Authorization of physical searches for foreign intelligence purposes.
Sec. 303. Application for an order.
Sec. 304. Issuance of an order.
Sec. 305. Use of information.
Sec. 306. Congressional oversight.
Sec. 307. Penalties.
Sec. 308. Civil liability.
Sec. 309. Authorization during time of war.

[1] In connection with this Act, see also section 107 of the Electronic Communications Privacy Act of 1986 regarding certain intelligence activities involving communications security, foreign power radio communications, and foreign power electronic communications systems; and see also section 2232 of title 18, United States Code, regarding prohibition on warning an individual of Foreign Intelligence Surveillance Act of 1978 surveillance. See also Communications Assistance for Law Enforcement Act, infra at p. 901.

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

Sec. 401. Definitions.
Sec. 402. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations.
Sec. 403. Authorization during emergencies.
Sec. 404. Authorization during time of war.
Sec. 405. Use of information.
Sec. 406. Congressional oversight.

TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES

Sec. 501. Access to certain business records for foreign intelligence and international terrorism investigations.
Sec. 502. Congressional oversight.

TITLE VI—OVERSIGHT

Sec. 601. Semiannual report of the Attorney General.
Sec. 602. Declassification of significant decisions, orders, and opinions.
Sec. 603. Annual reports.
Sec. 604. Public reporting by persons subject to orders.

TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES[2]

Sec. 701. Definitions.
Sec. 702. Procedures for targeting certain persons outside the United States other than United States persons.
Sec. 703. Certain acquisitions inside the United States targeting United States persons outside the United States.
Sec. 704. Other acquisitions targeting United States persons outside the United States.
Sec. 705. Joint applications and concurrent authorizations.
Sec. 706. Use of information acquired under title VII.
Sec. 707. Congressional oversight.
Sec. 708. Savings provision.

TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

Sec. 801. Definitions.
Sec. 802. Procedures for implementing statutory defenses.
Sec. 803. Preemption.
Sec. 804. Reporting.

# TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

## DEFINITIONS

SEC. 101. [50 U.S.C. 1801] As used in this title:

(a) "Foreign power" means—

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

[2] Section 403(b)(2)(A) of Public Law 110-261 (as amended) provides that effective December 31, 2017, the items relating to title VII in the table of contents are repealed.

(1) the total number of applications made for orders approving the use of pen registers or trap and trace devices under this title;

(2) the total number of such orders either granted, modified, or denied;

(3) the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 403, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices;

(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this title; and

(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).

## TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES[5]

### SEC. 501. [50 U.S.C. 1861] ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[5] Effective December 15, 2019, title V shall read as it read on October 25, 2001 pursuant to section 102(b)(1) of Public Law 109–177 (120 Stat. 195), as amended by section 1004(a) of division B of Public Law 111–118, section 1(a) of Public Law 111–141 (124 Stat. 37), section 2(a) of Public Law 112–3 (125 Stat. 5), section 2(a) of Public Law 112–14 (125 Stat. 216), and section 705(a) and (c) of Public Law 114–23 (129 Stat. 300), which appears up-to-date in another file (XML only). The provisions of title V of this Act prior to the enactment of Public Law 107–56 (and in effect on October 25, 2001) are shown in italic typeface following section 502.

Pursuant to Public Law 109–177, § 102(b)(1), as amended by Public Law 112–14, this section was amended, effective June 1, 2015, to read as it read on Oct. 25, 2001. The amendments made by Public Law 114–23, which was enacted June 2, 2015, were directed to this section as it read prior to such reversion and were executed as if the reversion had not taken place, to reflect the probable intent of Congress and the extension of the provisions of this section to Dec. 15, 2019, by Public Law 114–23, § 705(a), (c)

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a); or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2)[6] shall include—

(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

---

[Note: Effective on November 29, 2015, sections 101(a) and 103(a) of Public Law 114–23 provides for amendments to paragraph (2) of section 501(b). Upon such date, paragraph (2) reads as follows:]

*(2) shall include—*

[6] For version of law for section 501(b)(2), as amended by sections 101(a) and 103(a) of Public Law 114–23, see note below.

(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term "specific selection term" means a term that specifically identifies an individual, account, or personal device.

**SEC. 502. [50 U.S.C. 1862] CONGRESSIONAL OVERSIGHT.**[10]

(a) On an annual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate concerning all requests for the production of tangible things under section 501.

(b) In April of each year, the Attorney General shall submit to the House and Senate Committees on the Judiciary and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence a report setting forth with respect to the preceding calendar year—

(1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;

(2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;

(3) the total number of such orders either granted, modified, or denied;

(4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;

[10] For the expiration of section 502, see footnote set out at the beginning of title V.

(5) the total number of such orders either granted, modified, or denied;

(6) the total number of applications made for orders approving requests for the production of tangible things under section 501;

(7) the total number of such orders either granted, modified, or denied; and

(8) the number of such orders either granted, modified, or denied for the production of each of the following:

(A) Library circulation records, library patron lists, book sales records, or book customer lists.

(B) Firearms sales records.

(C) Tax return records.

(D) Educational records.

(E) Medical records containing information that would identify a person.

(c)(1) In April of each year, the Attorney General shall submit to Congress a report setting forth with respect to the preceding year—

(A) the total number of applications made for orders approving requests for the production of tangible things under section 501;

(B) the total number of such orders either granted, modified, or denied;

(C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;

(D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and

(E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).

(2) Each report under this subsection shall be submitted in unclassified form.

---

[Note: See footnote to the heading of title V. Sections 501 through 503 prior to the enactment of Public Law 107–56 are as follows:]

*DEFINITIONS*

*SEC. 501. [50 U.S.C. 1861] As used in this title:*

*(1) The terms "foreign power", "agent of a foreign power", "foreign intelligence information", "international terrorism", and "Attorney General" shall have the same meanings as in section 101 of this Act.*

*(2) The term "common carrier" means any person or entity transporting people or property by land, rail, water, or air for compensation.*

*(3) The term "physical storage facility" means any business or entity that provides space for the storage of goods or mate-*

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms "Foreign Intelligence Surveillance Court" and "Court" mean the court established under section 103(a).

(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms "Foreign Intelligence Surveillance Court of Review" and "Court of Review" mean the court established under section 103(b).

(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term "electronic communication service provider" means—

(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

(5) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

**SEC. 702. [50 U.S.C. 1881a] PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.**

(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) CONDUCT OF ACQUISITION.—

(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (g), such certification.

(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

(A) before the submission of a certification in accordance with subsection (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) TARGETING PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(e) MINIMIZATION PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

## 9.4. APÉNDICE D:

Fragmentos de la USA PATRIOT ACT [2001]

H. R. 3162

# One Hundred Seventh Congress of the United States of America

**AT THE FIRST SESSION**

***Begun and held at the City of Washington on Wednesday, the third day of January, two thousand and one***

## An Act

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:


Sec. 1. Short title and table of contents.
Sec. 2. Construction; severability.

TITLE I—ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 101. Counterterrorism fund.
Sec. 102. Sense of Congress condemning discrimination against Arab and Muslim Americans.
Sec. 103. Increased funding for the technical support center at the Federal Bureau of Investigation.
Sec. 104. Requests for military assistance to enforce prohibition in certain emergencies.
Sec. 105. Expansion of National Electronic Crime Task Force Initiative.
Sec. 106. Presidential authority.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.
Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
Sec. 203. Authority to share criminal investigative information.
Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
Sec. 205. Employment of translators by the Federal Bureau of Investigation.
Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.
Sec. 208. Designation of judges.
Sec. 209. Seizure of voice-mail messages pursuant to warrants.
Sec. 210. Scope of subpoenas for records of electronic communications.
Sec. 211. Clarification of scope.
Sec. 212. Emergency disclosure of electronic communications to protect life and limb.
Sec. 213. Authority for delaying notice of the execution of a warrant.
Sec. 214. Pen register and trap and trace authority under FISA.
Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.
Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications.
Sec. 218. Foreign intelligence information.
Sec. 219. Single-jurisdiction search warrants for terrorism.
Sec. 220. Nationwide service of search warrants for electronic evidence.
Sec. 221. Trade sanctions.
Sec. 222. Assistance to law enforcement agencies.
Sec. 223. Civil liability for certain unauthorized disclosures.
Sec. 224. Sunset.
Sec. 225. Immunity for compliance with FISA wiretap.

TITLE III—INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

Sec. 301. Short title.
Sec. 302. Findings and purposes.
Sec. 303. 4-year congressional review; expedited consideration.

Subtitle A—International Counter Money Laundering and Related Measures

Sec. 311. Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern.
Sec. 312. Special due diligence for correspondent accounts and private banking accounts.
Sec. 313. Prohibition on United States correspondent accounts with foreign shell banks.
Sec. 314. Cooperative efforts to deter money laundering.
Sec. 315. Inclusion of foreign corruption offenses as money laundering crimes.
Sec. 316. Anti-terrorist forfeiture protection.
Sec. 317. Long-arm jurisdiction over foreign money launderers.
Sec. 318. Laundering money through a foreign bank.
Sec. 319. Forfeiture of funds in United States interbank accounts.
Sec. 320. Proceeds of foreign crimes.
Sec. 321. Financial institutions specified in subchapter II of chapter 53 of title 31, United States code.
Sec. 322. Corporation represented by a fugitive.
Sec. 323. Enforcement of foreign judgments.
Sec. 324. Report and recommendation.
Sec. 325. Concentration accounts at financial institutions.
Sec. 326. Verification of identification.
Sec. 327. Consideration of anti-money laundering record.
Sec. 328. International cooperation on identification of originators of wire transfers.
Sec. 329. Criminal penalties.
Sec. 330. International cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups.

Subtitle B—Bank Secrecy Act Amendments and Related Improvements

Sec. 351. Amendments relating to reporting of suspicious activities.
Sec. 352. Anti-money laundering programs.
Sec. 353. Penalties for violations of geographic targeting orders and certain record-keeping requirements, and lengthening effective period of geographic targeting orders.
Sec. 354. Anti-money laundering strategy.
Sec. 355. Authorization to include suspicions of illegal activity in written employment references.
Sec. 356. Reporting of suspicious activities by securities brokers and dealers; investment company study.
Sec. 357. Special report on administration of bank secrecy provisions.
Sec. 358. Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism.
Sec. 359. Reporting of suspicious activities by underground banking systems.
Sec. 360. Use of authority of United States Executive Directors.
Sec. 361. Financial crimes enforcement network.
Sec. 362. Establishment of highly secure network.
Sec. 363. Increase in civil and criminal penalties for money laundering.
Sec. 364. Uniform protection authority for Federal Reserve facilities.
Sec. 365. Reports relating to coins and currency received in nonfinancial trade or business.
Sec. 366. Efficient use of currency transaction report system.

Subtitle C—Currency Crimes and Protection

Sec. 371. Bulk cash smuggling into or out of the United States.
Sec. 372. Forfeiture in currency reporting cases.

in the case of a trap and trace device, the geographic limits of the trap and trace order.".

(b) AUTHORIZATION DURING EMERGENCIES.—Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(1) in subsection (a), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"; and

(2) in subsection (b)(1), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution".

**SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.**

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

**"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.**

"(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

"(2) An investigation conducted under this section shall—

"(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

"(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(b) Each application under this section—

"(1) shall be made to—

"(A) a judge of the court established by section 103(a); or

"(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

"(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

"(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

"(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

"(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

"(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

**"SEC. 502. CONGRESSIONAL OVERSIGHT.**

"(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

"(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

"(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

"(2) the total number of such orders either granted, modified, or denied.".

**SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.**

(a) GENERAL LIMITATIONS.—Section 3121(c) of title 18, United States Code, is amended—

(1) by inserting "or trap and trace device" after "pen register";

(2) by inserting ", routing, addressing," after "dialing"; and

(3) by striking "call processing" and inserting "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications".

(b) ISSUANCE OF ORDERS.—

(1) IN GENERAL.—Section 3123(a) of title 18, United States Code, is amended to read as follows:

"(a) IN GENERAL.—

"(1) ATTORNEY FOR THE GOVERNMENT.—Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government

## 9.5. APÉNDICE E:

Fragmentos de la FISA Amendments Act [2008]

H. R. 6304

# One Hundred Tenth Congress of the United States of America

**AT THE SECOND SESSION**

***Begun and held at the City of Washington on Thursday, the third day of January, two thousand and eight***

## An Act

To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008" or the "FISA Amendments Act of 2008".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:


Sec. 1. Short title; table of contents.

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Sec. 101. Additional procedures regarding certain persons outside the United States.
Sec. 102. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.
Sec. 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978.
Sec. 104. Applications for court orders.
Sec. 105. Issuance of an order.
Sec. 106. Use of information.
Sec. 107. Amendments for physical searches.
Sec. 108. Amendments for emergency pen registers and trap and trace devices.
Sec. 109. Foreign Intelligence Surveillance Court.
Sec. 110. Weapons of mass destruction.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

Sec. 201. Procedures for implementing statutory defenses under the Foreign Intelligence Surveillance Act of 1978.
Sec. 202. Technical amendments.

TITLE III—REVIEW OF PREVIOUS ACTIONS

Sec. 301. Review of previous actions.

TITLE IV—OTHER PROVISIONS

Sec. 401. Severability.
Sec. 402. Effective date.
Sec. 403. Repeals.
Sec. 404. Transition procedures.

# TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

**SEC. 101. ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES.**

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by striking title VII; and

(2) by adding at the end the following:

# "TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

**"SEC. 701. DEFINITIONS.**

"(a) IN GENERAL.—The terms 'agent of a foreign power', 'Attorney General', 'contents', 'electronic surveillance', 'foreign intelligence information', 'foreign power', 'person', 'United States', and 'United States person' have the meanings given such terms in section 101, except as specifically provided in this title.

"(b) ADDITIONAL DEFINITIONS.—

"(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

"(A) the Select Committee on Intelligence of the Senate; and

"(B) the Permanent Select Committee on Intelligence of the House of Representatives.

"(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms 'Foreign Intelligence Surveillance Court' and 'Court' mean the court established under section 103(a).

"(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms 'Foreign Intelligence Surveillance Court of Review' and 'Court of Review' mean the court established under section 103(b).

"(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means—

"(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

"(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

"(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

"(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

"(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

"(5) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

**"SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.**

"(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

"(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

"(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

"(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

"(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

"(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

"(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

"(c) CONDUCT OF ACQUISITION.—

"(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

"(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

"(B) upon submission of a certification in accordance with subsection (g), such certification.

"(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

"(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

"(A) before the submission of a certification in accordance with subsection (g); or

"(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

"(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title

for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

"(d) TARGETING PROCEDURES.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

"(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

"(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

"(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(e) MINIMIZATION PROCEDURES.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

"(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(f) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

"(A) compliance with the limitations in subsection (b); and

"(B) that an application for a court order is filed as required by this Act.

"(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

"(A) the congressional intelligence committees;

"(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

"(C) the Foreign Intelligence Surveillance Court.

"(g) CERTIFICATION.—

"(1) IN GENERAL.—

"(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

"(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for

## 9.6. APÉNDICE F:

Orden del Juez Roger Vinson a la compañía Verizon [2013]

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR 13-80

## SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production



Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- *Remainder of page intentionally left blank.* --

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

## 9.7. APÉNDICE G:

Fragmentos de la USA FREEDOM ACT [2015]

# Public Law 114–23
## 114th Congress

## An Act

June 2, 2015
[H.R. 2048]

To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015.
50 USC 1801 note.

**SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015" or the "USA FREEDOM Act of 2015".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Amendments to the Foreign Intelligence Surveillance Act of 1978.

TITLE I—FISA BUSINESS RECORDS REFORMS

Sec. 101. Additional requirements for call detail records.
Sec. 102. Emergency authority.
Sec. 103. Prohibition on bulk collection of tangible things.
Sec. 104. Judicial review.
Sec. 105. Liability protection.
Sec. 106. Compensation for assistance.
Sec. 107. Definitions.
Sec. 108. Inspector General reports on business records orders.
Sec. 109. Effective date.
Sec. 110. Rule of construction.

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

Sec. 201. Prohibition on bulk collection.
Sec. 202. Privacy procedures.

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

Sec. 301. Limits on use of unlawfully obtained information.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

Sec. 401. Appointment of amicus curiae.
Sec. 402. Declassification of decisions, orders, and opinions.

TITLE V—NATIONAL SECURITY LETTER REFORM

Sec. 501. Prohibition on bulk collection.
Sec. 502. Limitations on disclosure of national security letters.
Sec. 503. Judicial review.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

Sec. 601. Additional reporting on orders requiring production of business records; business records compliance reports to Congress.

Sec. 602. Annual reports by the Government.
Sec. 603. Public reporting by persons subject to FISA orders.
Sec. 604. Reporting requirements for decisions, orders, and opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.
Sec. 605. Submission of reports under FISA.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

Sec. 701. Emergencies involving non-United States persons.
Sec. 702. Preservation of treatment of non-United States persons traveling outside the United States as agents of foreign powers.
Sec. 703. Improvement to investigations of international proliferation of weapons of mass destruction.
Sec. 704. Increase in penalties for material support of foreign terrorist organizations.
Sec. 705. Sunsets.

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

Subtitle A—Safety of Maritime Navigation

Sec. 801. Amendment to section 2280 of title 18, United States Code.
Sec. 802. New section 2280a of title 18, United States Code.
Sec. 803. Amendments to section 2281 of title 18, United States Code.
Sec. 804. New section 2281a of title 18, United States Code.
Sec. 805. Ancillary measure.

Subtitle B—Prevention of Nuclear Terrorism

Sec. 811. New section 2332i of title 18, United States Code.
Sec. 812. Amendment to section 831 of title 18, United States Code.

**SEC. 2. AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.**

Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or a repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

# TITLE I—FISA BUSINESS RECORDS REFORMS

**SEC. 101. ADDITIONAL REQUIREMENTS FOR CALL DETAIL RECORDS.**

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)) is amended—

(1) in subparagraph (A)—

(A) in the matter preceding clause (i), by striking "a statement" and inserting "in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement"; and

(B) in clause (iii), by striking "; and" and inserting a semicolon;

(2) by redesignating subparagraphs (A) and (B) as subparagraphs (B) and (D), respectively; and

(3) by inserting after subparagraph (B) (as so redesignated) the following new subparagraph:

"(C) in the case of an application for the production on an ongoing basis of call detail records created before,

"(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

Applicability.

"(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.".

(b) EMERGENCY AUTHORITY.—Section 403 (50 U.S.C. 1843) is amended by adding at the end the following new subsection:

"(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).".

# TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

### SEC. 301. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION.

Section 702(i)(3) (50 U.S.C. 1881a(i)(3)) is amended by adding at the end the following new subparagraph:

"(D) LIMITATION ON USE OF INFORMATION.—

"(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

"(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.".

## 9.8. CRONOLOGÍA DE ACONTECIMIENTOS

13/06/
**1942**

**Creación de la Oficina de Servicios Estratégicos.**
Aglutinó las tareas en clave de espionaje y contrainteligencia secreta frente a las potencias del eje. El 20 de septiembre de 1945 será disuelta.

12/04/
**1945**

**Inicio de la Presidencia de Harry S. Truman.**
A cuatro meses del fin de la Segunda Guerra Mundial se convierte en el 33º Presidente de los Estados Unidos. Con él la inteligencia cambia de ser capaz de adaptarse a las amenazas, a ser capaz de prevenirlas.

08/
**1945**

**Comienzo del Programa *SHAMROCK*.**
Nombre en clave del programa especial de la *NSA* por medio del cual se interceptaban los telegramas internacionales gracias a la colaboración de las compañías *RCA Global*, *ITT World Communications* y *Western Union International*.

02/09/
**1945**

**Final de la II Guerra Mundial.**

05/03/
**1946**

**Impulso del Acuerdo UKUSA.**
Contraído originariamente entre la *STANCIB* (State-Army-Navy Communication Intelligence Board) norteamericana y el Consejo de Inteligencia de Londres, se adhieren Canadá en 1948 y Australia y Nueva Zelanda en 1956, constituyendo la estructura del *Club de los Cinco Ojos*.

26/07/
**1947**

**Firma de la *National Security Act*.**
Firmado por el Presidente Truman, es el documento que dota de personalidad, con nombre y apellidos, al aparato de inteligencia norteamericano. Como el propio texto indica, pretende: "*proporcionar un programa integral para la seguridad futura de los Estados Unidos*". Además, crea la figura del Consejo de Seguridad Nacional y del Secretario de Estado, como "*subdirector al Presidente en todos los asuntos relacionados con la seguridad nacional*" y confiere rango de Agencia por vez primera a la *CIA*, tras la supresión de la *OSS*.

20/05/
**1949**

**Creación de la *Armed Forces Security Agency* (*AFSA*).**
Creada dentro del marco de dependencia del Departamento de Defensa (dirigido por Louis A. Johnson), su objetivo consistía en canalizar las actividades de inteligencia vinculadas al Departamento, excepto las realizadas por los sevicios militares. Falta de operatividad.

10/08/
**1949**

**Enmienda de la *National Security Act*.**
La *National Security Act* original concibe ahora la dependencia de cada uno de los respectivos secretarios de los departamentos del Ejército, Armada y Fuerza Aérea al Secretario de Defensa, dotándole de mayor autoridad en la nueva comunidad de inteligencia. El secretario de defensa pasa de ser un mero asesor al segundo eslabón de mando en la cadena militar.

10/03/
**1950**

**Directiva Nº 9: *Communications Intelligence*.**
La Directiva, con la firma estampada de Truman, coronaba el sistema de inteligencia emergente tras la Segunda Guerra Mundial, adaptando los criterios de la *National Security Act* a la nueva Comunidad. El entorno de inteligencia era propicio dado el contexto bipolar de Guerra Fría, acrecentado con el inminente estallido de la Guerra de Corea (25 de junio de 1950 - 27 de julio de 1953).

**13/12/ 1951**

**Fin de la *AFSA*.**
Dos grandes razones explican su fracaso: el intento de centralizar el esfuerzo de las actividades de *COMINT*, lo que hizo emerger un cierto recelo en las Agencias y la falta de autoridad de su Director sobre los diferentes servicios militares. Con la reforma de Truman de 1951, desaparece.

**28/12/ 1951**

**Comienzo del Comité Brownell.**
Tras la elaboración de un memorándum inicial, se recoge el intento presidencial de crear una Junta de Inteligencia y constituir un Comité que marque los primeros pasos de lo que desde entonces se conocerá como la *National Security Agency*. Al frente se ubica a un abogado: George Borwnell.

**13/06/ 1952**

**Informe del Comité Brownell.**
Contemplando la independencia interdepartamental y la necesidad de sacrificar la *AFSA*, se erigió en una especie de Carta Magna en la coordinación y trabajo de las tareas de *COMINT* en manos de la *NSA*, destacando la necesidad de involucrar al aparato militar dentro de la Agencia para no cometer errores del pasado.

**24/10/ 1952**

**Memorándum de Truman sobre la Inteligencia.**
Como respuesta al informe Brownell, Truman elabora un segundo memorándum por medio del cual se procederá al asentamiento del nuevo organismo de inteligencia y se ejecutarán reformas estructurales necesarias para la integración de la *NSA*.

**29/12/ 1952**

**Reforma de la Directiva Nº 9: *Communications Intelligence*.**
Entre las prerrogativas, se reforma la Directiva Nº 9: "*Communications Intelligence*" y por medio de la cual se recogen y enumeran las incipientes funciones de la *NSA* así como de su Director.

**20/01/ 1953**

**Fin de la etapa Truman. Inicio de la Presidencia Eisenhower.**

**01/11/ 1955**

**Comienzo de la Guerra de Vietnam.**
El conflicto estalló con objeto de impedir la reunificación de Vietnam bajo un Gobierno comunista. Participó la República de Vietnam (Vietnam del Sur) con el apoyo de Estados Unidos y otras naciones, contra la guerrilla local del Frente de Liberación de Vietnam (*Viet Cong*) y el ejército de la República Democrática de Vietnam (Vietnam del Norte), respaldados por China y principalmente por la Unión Soviética.

**1956**

**Operatividad de *COINTELPRO*.**
Nutriéndose en gran parte de los traumas generados por el Macarthismo (entre 1950 y 1956) y el panóptico obsesivo de J. Edgar Hoover al frente de la Oficina, el *FBI* desarrolla su programa de contraespionaje interno conocido como *COINTELPRO*, con el objetivo de "*perturbar, desestabilizar, paralizar, destruir o de otra manera, neutralizar, los individuos y grupos políticos disidentes en los Estados Unidos*". Una vez dado a conocer, se considera uno de los desembocantes necesarios para la conformación del Comité Church.

29/10/
**1956**

**Conflicto del Canal de Suez.**
La Guerra del Sinaí, llamada también Crisis de Suez, o bien Guerra de Suez, fue una contienda militar librada sobre territorio egipcio en el año 1956, que implicó a la alianza militar formada por el Reino Unido, Francia e Israel contra Egipto. El motivo no fue otro que oponerse a la nacionalización del Canal por parte del Presidente de Egipto, Nasser. Los Estados Unidos y la URSS estaban en contra de la intervención de la triple alianza por distintas razones. Por ejemplo, los soviéticos se habían convertido en uno de los principales aliados de Siria, y buscaban incrementar su popularidad en el mundo árabe.

20/01/
**1961**

**Fin de la etapa Eisenhower. Inicio de la Presidencia Kennedy.**

15/04/
**1961**

**Incidente en Bahía de Cochinos.**
Tras el triunfo de la Revolución Socialista cubana en 1959, el Gobierno de Castro se aproximó al de la URSS, lo que unido a la ubicación de misiles balísticos nucleares en la costa de Bahía de cochinos, incentivó a las tropas americanas a invadir la isla. La acción acabó en fracaso. En menos de 65 horas, fue completamente aplastada por las Fuerzas Armadas Revolucionarias (*FAR*) de Cuba. Después, se procedería al desarme de los misiles, pero la tensión no se rebajaría.

06/09/
**1961**

**Nacimiento de la *National Reconnaissance Office.***
Casi veinte años después del ataque japonés a Pearl Harbor, el Director de la *CIA*, el general Charles Cabell, estableció el 6 de septiembre de 1961 el memorándum Roswell Gilpatric, por el que nace la *National Reconnaissance Office* (*NRO*), en un afán de despejar los fantasmas del pasado y con la esperanza de que, por medio de tecnología satelital y la agrupación de un equipo de científicos de gran formación, Estados Unidos nunca tendría que volver a enfrentarse a sorpresas tan devastadoras.

22/11/
**1963**

**Fin de la etapa Kennedy. Inicio de la Presidencia Lyndon B. Johnson.**

**1969**

**Comienzo de la operatividad de *MINARET.***
En 1969, la *NSA* formalizó el programa *MINARET*, con el que se daba comienzo a la elaboración de las listas de vigilancia. El proyecto fue el resultado de una campaña iniciada en el otoño de 1967, cuando se creó la *Civil Disturbance Unit*. El programa no sólo se aplicaba, según reconocía el informe del Comité Church, a la influencia extranjera sobre la disidencia interna sino también a los "*grupos e individuos americanos cuyas actividades podían dar lugar a disturbios civiles u otra manera de subvertir la seguridad nacional de los Estados Unidos*".

**20/01/**
**1969**

**Fin de la etapa Johnson. Inicio de la Presidencia Nixon.**

**23/12/**
**1971**

**Creación por Directiva presidencial del *Central Security Service* (*CSS*).**

Un organismo pensado para promover la colaboración y combinación entre la *NSA* y los órganos de inteligencia de las Fuerzas Armadas especializadas en procedimientos criptográficos y reforzado bajo la dirección de la misma persona para ambas Agencias. En la Directiva de 1971 se detalla con claridad el papel de la *NSA* como organización encargada de las tareas de Señales de Inteligencia (*SIGINT*) y del propio *CSS* como herramienta de soporte.

**24/03/**
**1971**

***The Washington Post* revela *COINTELPRO*. Fin de operatividades.**

De acuerdo a las líneas oficiales de investigación, *COINTELPRO* tuvo una vigencia de quince años, entre 1956 y 1971. Durante este tiempo, el *FBI* admitió haber participado en 2.218 operaciones junto con otro tipo de prácticas, hoy más frecuentes, como la escucha telefónica sin orden judicial y la interceptación de la correspondencia con la colaboración de la *CIA*.

**13/06/**
**1971**

**Primera publicación sobre los *Pentagon Papers* facilitados por Daniel Ellsberg a *The New York Times*.**

*The New York Times* publicó la primera serie de archivos que había recibido de Ellsberg bajo el titular: "*Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement*". En la serie se revelaba cómo Ellsberg había comenzado el 1 de octubre de 1969 a hacer copias de los documentos, para demostrar que la participación de Estados Unidos en la Guerra de Vietnam se basaba en dos décadas de mentiras y de crímenes de guerra.

**17/07/**
**1972**

**Revelación del *WATERGATE*.**

*The Washington Post* reveló el escándalo *Watergate*, en el que el Ejecutivo había dirigido la inteligencia nacional para llevar a cabo operaciones de espionaje constitucionalmente cuestionables. Los intentos de espiar e intervenir las comunicaciones del Partido Demócrata dinamitaron la carrera de Nixon como Presidente.

**09/**
**1973**

**Fin del proyecto *MINARET* por el director de la *NSA*, el General Lew Allen, Jr.**

El entonces Director de la *NSA*, el General Lew Allen, Jr. suspendió el programa y reconoció la autoría de la Agencia detrás de las listas de vigilancia.

09/10/
**1974**

**Fin de la etapa Nixon. Inicio de la Presidencia Ford.**

21/01/
**1975**

**Resolución para la conformación del Comité Church.**

El senador John Pastore presentó la Resolución donde se conformaba este Comité especial, bajo presidencia de Frank Church (senador demócrata por Idaho) y con John Tower como Vicepresidente (senador republicano por Texas). Concebido para durar doce meses, aunque se prologara hasta los dieciséis, contrató alrededor de 150 funcionarios peinando más de 100.000 documentos clasificados y no clasificados y entrevistó a 800 personas, incluidos exdirectores de la *CIA*.

30/04/
**1975**

**Fin de la Guerra de Vietnam.**

05/
**1975**

**Fin de operatividades del programa *SHAMROCK*.**

En la expansión del programa fue esencial la cooperación de Agencias de comunicaciones transnacionales, como era el caso de *RCA Global*, *ITT World Communications* y *Western Union International*. Aunque el número total de telegramas interceptados y leídos no es oficial, la *NSA* estima que en los últimos dos años de operatividad del programa fueron revisados un total de 150.660 telegramas.

**1975**

***Church Committee*. [Comité Selecto del Senado de los Estados Unidos para el Estudio de las Operaciones Gubernamentales Respecto a las Actividades de Inteligencia].**

Los investigadores concluyeron que desde la administración del Presidente Franklin D. Roosevelt y hasta la década de los setenta, los excesos de vigilancia tanto dentro como fuera de las fronteras estadounidenses, se debían al ascenso norteamericano en el ejercicio de una superpotencia en plena confrontación bipolar, en el contexto de la Guerra Fría. También destacó en su informe final la falta de ensamblaje y coordinación entre el *FBI* y la *CIA* desacreditando por tanto el papel del llamado Plan *Huston*, y sentó las bases para la aprobación de la futura *Foreign Intelligence Surveillance Act* (*FISA*) ratificada en 1978, y firmada por el Presidente Jimmy Carter.

20/01/
**1977**

**Fin de la etapa Ford. Inicio de la Presidencia Carter.**

07/
**1977**

**Algoritmo *Data Encryption Standard.***

La *NSA* comenzó a trabajar en su propio algoritmo de cifrado, aunque la colaboración entre Howard Rosenblum, subdirector de investigación e ingeniería, y Walter Tuchman, de *IBM*, fue clave para alcanzar el éxito. En julio de 1977, el algoritmo *Data Encryption Standard* era ya una realidad.

26/08/
**1977**

**Tratado de paz de *CIA* con *NSA* impulsado por el Director de la *NSA*, Bobby Inman.**

Se lanza el "*tratado de paz*" entre las Agencias *NSA* y *CIA* con mediación del Director de la *NSA* Bobby Inman, quien coincidiendo con la llegada a la Presidencia de Jimmy Carter (1977-1981); releva al frente de la Agencia al General Lew Allen. El acuerdo confería, con objeto de evitar futuras colisiones, que el agente centralizador de las tareas de *SIGINT* será la *NSA*.

25/10/
**1978**

**Impulso de la *Foreign Intelligence Surveillance Act* y del Tribunal *FISA*.**

Una articulación jurídica que, en origen no se aplicaba fuera de territorio estadounidense y que regulaba los procesos para desarrollar una estrecha vigilancia tanto física como electrónica, y las funciones pertinentes de recopilación de información. Para poder imponer o acatar los preceptos de la Ley, el Comité decidió dotarle de su brazo ejecutor, el *Foreign Intelligence Surveillance Court* (*FISC*), como organismo concebido para la interpretación de la Ley y su cumplimiento así como elemento de concesión fundamental para las Agencias a la hora de obtener permisos de vigilancia, incluso cuando el objetivo solicitado en cuestión se encontrase fuera de Estados Unidos.

20/01/
**1981**

**Fin de la etapa Carter. Inicio de la Presidencia Reagan.**

04/12/
**1981**

**Firma de la Orden Ejecutiva *12333*.**

El 4 de diciembre de 1981, el Presidente Ronald Reagan firmaba la Orden Ejecutiva *12333*, por la que se actualizaba la estructura de la Comunidad de Inteligencia norteamericana en su conjunto. La Orden sentó las bases sobre las que actuar en plena espiral de confrontación y la orientación de los esfuerzos de inteligencia, además de reconocer las amenazas principales y distinguir en el espionaje, el terrorismo y las armas de destrucción masiva los núcleos de acción fundamentales.

19/11/
**1985**

**Cumbre de Ginebra.**

La cumbre marcó el comienzo del deshielo de las relaciones soviético-estadounidenses tipificadas entre Mijaíl Gorbachov y Ronald Reagan. Aunque en el comienzo de las conversaciones, el Presidente norteamericano se negara a dar marcha atrás en sus ambiciosos planes militarizadores, bautizados como "*la guerra de las galaxias*", el camino no conduciría sino al deshielo definitivo de las tensiones, con el acuerdo *START I* en la cumbre de Moscú de 1989. Un paso definitivo y previo necesario, para la declaración conjunta entre el sucesor de Reagan, George H. W. Bush, y el propio Gorbachov, el 3 de diciembre de 1989, en la cumbre de Malta, en la que se daba por zanjada la Guerra Fría.

01/10/
**1986**

**Firma de la *Goldwater-Nichols Reorganization Act.***

A partir de la *Goldwater-Nichols Act* de 1986, de reorganización del DoD, el establecimiento militar sufrió el conjunto más radical de reformas en materia de defensa en casi 40 años de existencia. La *Goldwater-Nichols Act* en su preámbulo, ya dejaba claro su propósito de reorganización del DoD para el fortalecimiento de la autoridad civil en detrimento de la propiamente militar y la mejora en el asesoramiento militar al Presidente y al *National Security Council*.

12/08/
**1988**

**Revelación de *ECHELON* en *The New Statesman*.**

Creado a finales de los sesenta con el objetivo de supervisar las comunicaciones militares y diplomáticas de la URSS y sus aliados del bloque del este en el contexto de la Guerra Fría. El programa fue revelado en 1988 en la revista británica *The New Statesman* por el periodista de investigación Duncan Campbell, quien también fue el encargado de elaborar en 1999 el Informe Interception Capabilities 2000 para el Parlamento Europeo, donde se desgrana el funcionamiento de *ECHELON* y su impacto sobre *COMINT*.

20/01/
**1989**

**Fin de la etapa Reagan. Inicio de la Presidencia George H. W. Bush.**

10/11/
**1989**

**Caída del Muro de Berlín.**

03/12/
**1989**

**Celebración de la Cumbre de Malta.**

Consistió en una reunión entre los Presidentes de los Estados Unidos, George H. W. Bush y la Union Soviética, Mijail Gorbachov, que tuvo lugar durante los días 2 y 3 de diciembre de 1989, pocas semanas después de la caída del Muro de Berlín. Su principal objetivo era reunir a las dos superpotencias para que tuvieran la posibilidad de discutir los cambios que se estaban produciendo en Europa tras la caída del Telón de Acero. La cumbre para algunos observadores era el principio del fin de la Guerra Fría.

02/08/
**1990**

**Guerra del Golfo Pérsico.**

Desde el enfoque puramente militar, la victoria norteamericana en la guerra del golfo pérsico, iniciada en agosto de 1991 y finalizada en febrero de 1992, puso de manifiesto el prototipo de guerra para el futuro. De este modo, la rápida victoria en el conflicto de la coalición liderada por Estados Unidos sugiere la puesta en marcha de una *Revolution in Military Affairs* (*RMA*), resultado de la expansión del sector en la etapa Reagan.

25/12/
**1991**

**Caída de la URSS.**

Después de que la Comunidad de Estados Independientes solicitara la disolución definitiva de la URSS en el Tratado de Belavezha, Gorbachov renunció a su cargo y la Unión Soviética dejó de existir formalmente el 25 de diciembre de 1991. El Soviet Supremo reconocería al día siguiente la extinción de la Unión. A partir de ese momento, el causante de la disolución, Yeltsin, daría comienzo al nuevo proyecto de Rusia bajo su liderazgo político.

**20/01/ 1993**

**Fin de la etapa H. W. Bush. Inicio de la Presidencia Clinton.**

**12/ 1999**

**Wen Ho Lee es acusado de transferir secretos nucleares a China.**

Un científico nuclear que trabajaba para la Universidad de California en el laboratorio nacional Los Álamos, dependiente del Departamento de Energía, quien fue acusado de espionaje y aportación de datos sobre el arsenal nuclear estadounidense a la República Popular de China en diciembre de 1999.

**20/01/ 2001**

**Fin de la etapa Clinton. Inicio de la Presidencia George W. Bush.**

**11/07/ 2001**

**Parlamento Europeo. Comisión temporal sobre el sistema de interceptación *ECHELON*.**

Inició una investigación que acabaría demostrando la existencia de este programa, que operaba bajo la "*cooperación proporcionada entre los Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda, es decir, en el marco del Acuerdo UKUSA, para interceptar comunicaciones privadas y comerciales, así como las comunicaciones no militares*".

**28/08/ 2001**

**Rastreo de e-mails de Moussaoui.**

Ya en el año 1990 Coleen Rowley asumió el cargo de Jefe de la División de Asesoría del *FBI* en Minneapolispone el punto de mira en Zacarias Moussaoui, quien luego fuera arrestado por participar activamente en la serie de atentados. A pesar de solicitar de forma cautelar una custodia que fue denegada, tampoco el personal cualificado del *FBI* difundió las sospechas a otras autoridades internas de la Agencia, lo que facilitó la dispersión y el olvido.

**11/09/ 2001**

**Ataque terrorista al World Trade Center.**

El 11 de septiembre de 2001 permanece en el imaginario colectivo como el acontecimiento más impactante y el acto de bienvenida más dramático del nuevo siglo. La configuración geoestratégica mundial, con el comienzo de la *"Global War on Terror"*, (*GWOT*) la reordenación de las amenazas internacionales y lo más importante, la sensación global de que el estandarte más seguro del mundo se podía ver atacado, se constituyeron rápidamente en las creencias extendidas y en los pilares que cercaban la seguridad del siglo XXI.

**04/10/ 2001**

**Inicio de *STELLARWIND*.**

Según William Binney, cripto-matemático en la *NSA* durante la Guerra Fría, todo su trabajo basado en la relación de datos y metadatos sociales para el impulso de una base de datos electrónica de correlaciones, adquirió un cariz de espionaje masivo tras el ataque del 11 de septiembre. El programa resultante, llamado *STELLARWIND*, fue reautorizado cada 45 días por el conocido por Binney como el "*Comité del sí*": Comité formado por Hayden, Tenet y el Departamento de Justicia.

**26/10/ 2001**

**Firma de la USA PATRIOT ACT.**

Todavía con el trauma de los devastadores acontecimientos, el espíritu de la Ley, como señala Gustavo Díaz Matey, la *USA PATRIOT ACT* consistió en una "*disminución de la capacidad de los ciudadanos estadounidenses para obtener información sobre su Gobierno y, al mismo tiempo, le dio al Gobierno los medios para husmear en la vida personal de los mismos ciudadanos*".

**2002**

**Comienzo del monitoreo masivo autorizado por el Presidente Bush bajo pretensión de Hayden, y del vicepresidente Cheney.**

Bajo iniciativa personal de su Vicepresidente primero Dick Cheney y Michael Hayden al frente de la *NSA*, a monitorizar, almacenar y analizar sin orden judicial previa, las llamadas telefónicas y los correos electrónicos de aquellos ciudadanos, estadounidenses o no, sospechosos de tener algún nexo con Al-Qaeda.

**05/ 2002**

**Coleen Rowley testifica ante el Comité Judicial del Senado.**

En mayo de 2002, Rowley testificó ante el Comité Judicial del Senado sobre los acontecimientos que derivaron en el ataque terrorista del 11-S-. A la vez que ejercía su derecho a declarar, Rowley hizo pública una carta dirigida al Director del *FBI*, Robert Mueller, donde justificaba su declaración. En ella, Rowley pone el punto de mira en Zacarías Moussaoui, quien luego fuera arrestado por participar activamente en la serie de atentados.

**19/11/ 2003**

**Documento *"FAIRVIEW y STORMBREW: en vivo – en la red"*.**

La *NSA* se jacta de que, al poco de su puesta en marcha, estos programas, consiguieron en un esfuerzo por modernizar las tareas de registros DNR y DNI, hasta cuadriplicar la producción de señales *SIGINT*. De la misma forma, se reconoce la gran prestación de *STORMBREW* al dotarse de una Capacidad de Reacción Rápida.

**17/12/ 2004**

***Intelligence Reform and Terrorism Prevention Act.***

Un texto que persigue la reforma de la estructura de la Comunidad de Inteligencia bajo la nueva figura del *Director of National Intelligence*. De la misma manera, el texto diferencia bajo las competencias de su cargo, en un primer nivel, entre el *National Counterterrorism Center (NCTC), la Privacy and Civil Liberties Oversight Board (PCLOB) y el National Counterproliferation Center (NCPC)*.

**2005**

**Demanda el ex técnico de *AT&T* Mark Klein.**

Mark Klein, ex técnico de *AT&T* fue testigo clave en la demanda colectiva que presentó *Electronic Frontier Foundation* en contra de la compañía, alegó la cooperación ilegal entre *AT&T* y la *NSA*, en base a la disposición de un engranaje de vigilancia para espiar el tráfico de Internet. El entramado, sobre todo, respondía a la conocida como estructura del "*secret room*" que era la plataforma Narus STA 6400.

**2005**

***AT&T*: absorción de *SBC Communications*.**

Lo que hizo que se expandiera la cuota de mercado del Grupo, la encargada de las telecomunicaciones, según Greenwald, posibilitó de acuerdo con los archivos de la *NSA* "*en 2010 una lista de países seleccionados por BLARNEY que incluía Brasil, Alemania, Grecia, Israel, Italia, Japón, México, Corea del Sur y Venezuela así como la Unión Europea y las Naciones Unidas*".

07/
**2005**

**Revisión del Senado de la *USA PATRIOT ACT.***
En la revisión de 2005, se garantizó el endurecimiento de la Ley en materia de recopilación de metadatos en manos de los servicios de inteligencia. Mediante la renovación de 2005, a pesar de la prohibición marcada por la Cuarta Enmienda a la hora de ejercer registros e incautaciones de modo indiscriminado, el Senado garantizó una mayor protección a las prácticas de las Agencias.

**2006**

**Fin del proyecto *TRAILBLAZER.***
El programa en cuestión, dependiente de la *NSA*, consistía en un sistema avanzado de análisis de datos mediante rastreo de comunicaciones como Internet, además de contemplar facetas de seguimiento por medio de filtrado de correos electrónicos y localización telefónica.

16/03/
**2006**

**Introducción en la Ley *FISA* de la *Terrorist Surveillance Act.***
Los senadores Mike DeWine, Lindsey Graham, Chuck Hagel y Olympia Snowe la introdujeron en la propia Ley. Con este primer reajuste, se dotaba al Presidente de una autoridad adicional para llevar a cabo las actividades de vigilancia electrónica de presuntos terroristas sujetos a la supervisión del Estado e incluidos en las listas de vigilancia como potenciales amenazas.

11/15/
**2006**

***USA TODAY* da a conocer la cooperación entre *AT&T, Verizon* y *BellSouth* con la *National Security Agency.***
La periodista del *USA Today*, Leslie Cauley, dio a conocer la cooperación entre las compañías *AT&T, Verizon y BellSouth* con la *National Security Agency* para acceder en secreto a los registros telefónicos de millones de ciudadanos estadounidenses, bajo el titular: *"La NSA posee una base de datos masiva de llamadas telefónicas de estadounidenses".*

18/07/
**2006**

**Introducción en la Ley *FISA* de la *Electronic Surveillance Modernization Act.***
La senadora Heather Wilson introdujo este texto que aumentaba la autoridad presidencial hasta convertirle, por medio de la Fiscalía General en el centro de la vigilancia electrónica sin necesidad de previa orden judicial, de toda la actividad derivada de las llamadas telefónicas internacionales y el correo electrónico de grupos armados terroristas identificados en previsión de posibles amenazas a la nación.

12/
**2006**

**Lanzamiento de la plataforma *WIKILEAKS.***
*WikiLeaks* se ha erigido, desde el comienzo del nuevo siglo, en el estandarte de las filtraciones en lo que respecta al contingente de operaciones implementadas por el Gobierno norteamericano en respuesta a los ataques del 11 de septiembre de 2001. La importancia de *WikiLeaks* en materia de filtraciones supone un punto de inflexión que sin duda estimula a numerosas fuentes a la denuncia de sus Gobiernos, como sucederá años más tarde, con Snowden.

**2007**

**Comienza *PRISM.***
El programa más ambicioso de todos, puesto que permite a la *NSA* obtener prácticamente cualquier información de las empresas de Internet, que centenares de millones de personas de todo el mundo utilizan hoy como principal medio de comunicación. Las empresas de Internet que, según los documentos de la *NSA*, proporcionaban a la Agencia acceso directo a sus servidores como parte de *PRISM* eran: *Facebook, Google, Apple, YouTube y Skype*, entre otras.

13/06/
**2007**

**Thomas Drake es acusado de ser enemigo del Estado.**
Ex alto cargo de la *National Security Agency*. Entre las acusaciones, la extracción de documentos de la sede de la Agencia en Fort Meade, Maryland, con el propósito de filtrarlos a la prensa e informar así acerca de las dudosas prácticas jurídicas puestas en marcha por la Agencia bajo la coartada de su campaña contra el terrorismo. En su defensa, Drake aludió a Michael Hayden, Director de la *CIA* entre 2006 y 2009, que perseguía silenciarle por su oposición al proyecto *TRAILBLAZER*.

28/07/
**2007**

**Introducción en la Ley *FISA* de la *Protect America Act*.**
Con esta incorporación a la Ley *FISA*, se pretendía que la propia estructura legal amparase al Gobierno a intervenir las comunicaciones extranjeras sin supervisión del Tribunal *FISA*.

08/12/
**2007**

**Inicio de *SHELLTRUMPET*.**
Comenzó el 8 de diciembre de 2007 como un analista de metadatos casi en tiempo real para un sistema de recogida clásico, tal como indica un documento filtrado de la *NSA* de alto secreto en el que se reconocen las ventajas del programa, así como el salto en la recogida de datos. Según Greenwald, "*cinco años después [el programa] está procesando dos mil millones de incidentes/día y otros sistemas de la Agencia han llegado a utilizar sus capacidades de procesamiento*".

01/
**2008**

***Comprehensive National Cybersecurity Initiative*.**
Para fomentar un enfoque múltiple en la identificación de las emergentes amenazas cibernéticas, apuntalar las telecomunicaciones actuales y futuras, y detectar las vulnerabilidades cibernéticas, con objeto de hacer frente de forma proactiva a las entidades que desean robar o manipular los datos protegidos en los sistemas federales de seguridad.

**2008**

**Inicio de *TEMPORA*.**
Con *TEMPORA*, el *GCHQ* tiene la capacidad para acceder a grandes cantidades de datos, extraídos de los cables de fibra óptica y almacenarlos durante 30 días, para que puedan ser cribados y analizados. Teniendo siempre en cuenta que, si bien la mayoría del flujo informativo o de datos, en algún momento ha de pasar por los cables de Estados Unidos, en el continente europeo, ese papel lo ejerce el Reino Unido, concentrando la mayor presencia de cables submarinos de fibra óptica de tránsito de datos de toda Europa.

12/03/
**2008**

**Adhesión de *Yahoo* a *PRISM*.**

20/06/
**2008**

**Aprobación de la *FISA Amendments Act*.**
Como indicó el senador Wyden, en el Comité de Investigación sobre la *FISA* Amendments Act de 2008, la nueva Sección 702, no implicaba la mera obtención de registros individuales, sino que le permitía al Gobierno "*obtener órdenes programáticas que duran un año entero y le autorizan a recoger un número potencialmente elevado de llamadas telefónicas y mensajes de correo electrónico, sin necesidad de que los remitentes o destinatarios estén realmente conectados con el terrorismo o el espionaje*".

**14/01/ 2009**

**Adhesión de *Google* a *PRISM*.**

**20/01/ 2009**

**Fin de la etapa Bush. Inicio de la Presidencia Barack Obama.**

**03/ 2009**

**Comienzo de herramienta *ORANGECRUSH*.**

Subprograma de *OAKSTAR*. En un documento revelado se establece la participación del Gobierno de Polonia como intermediario para facilitar el envío masivo de datos bajo la herramienta *ORANGECRUSH*, aunque el servicio de inteligencia polaco lo conoce bajo el nombre en clave *BUFFALOGREEN*. Al mismo tiempo, el documento establece el gran paso adelante en la recolección de metadatos que va a significar el subprograma, gracias siempre a los enlaces comerciales gestionados por el socio corporativo de la *NSA*.

**03/06/ 2009**

**Adhesión de *Facebook* a *PRISM*.**

**11/11/ 2009**

**Aparece en un documento el nombre de *SILVERZEPHYR* como socio corporativo de *OAKSTAR*.**

El programa *OAKSTAR* aprovecha el acceso de uno de los socios corporativos de la Agencia (nombre en clave *STEELKNIGHT*) a los sistemas extranjeros de telecomunicaciones, empleando este acceso para desviar datos a sus propios almacenes. Mientras, otro socio, *"(nombre en clave: SILVERZEPHYR) aparece en un documento del 11 de noviembre de 2009 que describe la labor realizada con la empresa para obtener "comunicaciones internas" de Brasil y Colombia"*.

**07/12/ 2009**

**Adhesión de *PalTalk* a *PRISM*.**

**05/04/ 2010**

***Baghdad Airstrike.***

A las 10:44 horas del 5 de abril de 2010, *WikiLeaks* hacía público un vídeo correspondiente a información militar clasificada en el que se observa el asesinato de más de una docena de personas en el suburbio iraquí de Nueva Baghdad, contando entre ellos a Namir Noor-Eldeen y su ayudante, dos empleados de la Agencia *Reuters*, que se encontraban en el terreno realizando labores periodísticas.

**25/07/ 2010**

***Afghanistan war logs.***

El 25 de julio de 2010, *WikiLeaks* hacía públicos los casi 77.000 registros acaecidos durante la guerra de Afganistán entre enero de 2004 y diciembre de 2009. El conocido como diario de la guerra de Afganistán detalla cada una de las acciones militares letales o no letales que implican a militares estadounidenses.

**24/09/ 2010**

**Adhesión de *YouTube* a *PRISM*.**

**22/10/ 2010**

***Iraq War Logs.***

El 22 de octubre de 2010, *WikiLeaks* publicó la filtración de información clasificada militar más importante de la historia: 391.832 informes que documentaban los sucesos de la guerra de Irak desde el 1 de enero de 2004 al 31 de diciembre de 2009 (excepto los meses de mayo de 2004 y marzo de 2009). En los informes se detallan hasta 109.032 muertes, de las cuales 66.081 corresponden a civiles y 23.984 al catalogado como grupo insurgente.

**28/11/ 2010**

***Cablegate.***

El 28 de noviembre de 2010, *WikiLeaks* hacía públicos un total de 251.287 cables de información confidencial de las diferentes embajadas norteamericanas. Los cables, que contienen información desde 1966 hasta febrero de 2010, revelan documentos públicos concernientes al total de 274 embajadas, consulados y misiones diplomáticas en países de todo el mundo. Un global de 261.276.536 palabras, siete veces más que el tamaño de los documentos relativos a la guerra de Irak.

**06/02/ 2011**

**Adhesión de *Skype* a *PRISM*.**

**31/03/ 2011**

**Adhesión de *AOL* a *PRISM*.**

**27/02/ 2012**

***Global Intelligence Files leak.***

El 27 de febrero de 2012, *WikiLeaks* publicó más de cinco millones de correos electrónicos de la empresa de inteligencia global, con sede en Texas: *Stratfor*. Los correos datan del período comprendido entre julio de 2004 y finales de diciembre de 2011. Los correos demuestran que la compañía ofrece sus servicios de inteligencia confidencial a grandes corporaciones dependientes del Gobierno norteamericano, entre ellas, el propio el *US Department of Homeland Security* (Departamento de Seguridad Nacional).

**10/ 2012**

**Adhesión de *Apple* a *PRISM*.**

**20/05/ 2013**

**Llegada de Snowden a Hong Kong.**

Después de haber trabajado como analista para la *NSA* desde 2010, en empresas contratistas como *Dell Corporation* o *Booz Allen Hamilton*, solicita un permiso el 20 de mayo de 2013 para recibir tratamiento contra la epilepsia y llega a Hong Kong, donde no sin tenerlo todo previsto contacta con los periodistas Glenn Greenwald y Laura Poitras.

**06/06/ 2013**

**Primer encuentro con Edward Snowden.**

El ex analista de la *NSA*, Edward Snowden, por fin veía cara a cara a Glenn Greenwald, el informador del diario *The Guardian*, a quien había decidido confiar las revelaciones que estarían a punto de hacer tambalear los cimientos de la Comunidad de Inteligencia norteamericana. El escenario, el Hotel Mira de Hong Kong.

**07/06/ 2013**

**Revelación de *PRISM*.**

El programa posibilita a los analistas de la *NSA* la recogida de material en bruto, incluidos los historiales de búsqueda, correos electrónicos, contenido de mensajes, chats en vivo o las transferencias de archivos, de acuerdo con la publicación del diario *The Guardian* del 7 de junio de 2013, momento en que el programa de vigilancia sale a la luz, gracias a las filtraciones de Edward Snowden y los periodistas Glenn Greenwald y Ewen MacAskill.

**08/06/ 2013**

**El Parlamento Europeo decide crear la Comisión de Libertades Civiles.**

Con la que se pretendió llevar a cabo una investigación a fondo de los programas de vigilancia de Estados Unidos. Además de obtener un respaldo masivo en la propia puesta en marcha de la Comisión, los eurodiputados manifestaron su condena enérgica a las técnicas de espionaje, a la vez que pedían a Estados Unidos argumentos para defenderse de las acusaciones.

**11/06/ 2013**

**Revelación de *BOUNDLESS INFORMANT*.**

El 11 de junio de 2013, *The Guardian*, de la mano de los periodistas Glenn Greenwald y Ewan MacAskill, hacía público el programa *BOUNDLESS INFORMANT*, una herramienta interna de la *NSA* cuyo objetivo no se encuentra tanto en escudriñar el contenido de un email o un mensaje, sino en la relación de metadatos.

**23/06/ 2013**

**Huida de Snowden a Moscú.**

Snowden huyó hacia Rusia el 23 de junio de 2013 y tras pasar cinco semanas en la zona de tránsito del aeropuerto Sheremetievo de Moscú, finalmente el 1 de agosto de 2013, el Gobierno le concedió el derecho de asilo por un año.

**27/06/ 2013**

**Revelación de *SHELLTRUMPET*.**

El 27 de junio de 2013, el propio Greenwald y el periodista Spencer Ackerman, hacían público el programa en *The Guardian*, bajo el titular: *"How the NSA is still harvesting your online data"*.

**07/07/ 2013**

**Revelación de *FAIRVIEW*.**

En el diario brasileño *O Globo*, el propio Greenwald, en colaboración con los también periodistas Roberto Kaz y José Casado, revelaban a la opinión pública los entresijos del programa *FAIRVIEW* bajo el titular: *"Estados Unidos espía millones de emails y llamadas telefónicas de brasileños"*. En la información se destacaba que, en el mes de enero del mismo año, Brasil se convirtió en uno de los países más espiados por la *NSA* tras los Estados Unidos, con un registro total de cerca de 2,3 millones de llamadas y correos espiados.

**19/07/ 2013**

**Se hace pública la orden del juez Vinson obligando a *Verizon Communications* a ceder información de sus clientes a la *NSA*.**

Se obligaba a *Verizon* a facilitar las copias electrónicas de *"todos los registros detallados de llamadas o metadatos de telefonía creados por Verizon para las comunicaciones entre los Estados Unidos y en el extranjero o totalmente dentro de los Estados Unidos, incluyendo llamadas telefónicas locales"*.

**31/07/ 2013**

**Revelación de *X-KEYSCORE*.**

En el artículo publicado por el propio Greenwald en *The Guardian* el 31 de julio de 2013, donde se informa a la opinión pública por vez primera acerca de la existencia de *X-Keyscore*, Snowden reconoce la facilidad de acceso a la privacidad de los ciudadanos mediante esta herramienta con tan sólo el conocimiento de una cuenta de email, se encuentra presente en 150 países, si atendemos a que en total en el mundo hay 194 países, esto significa que *X-Keyscore* proporciona datos de inteligencia del 79,3% del territorio mundial.

**01/08/ 2013**

**Concesión de Moscú a Snowden de un derecho de asilo por un año.**

**08/ 2013**

**Bradley Manning condenado a 35 años de prisión.**

Por ser considerado el responsable de filtrar miles de cables clasificados a *WikiLeaks*. Entre las filtraciones, el suceso conocido como *"Collateral Murder"* o los diarios de la Guerra de Afganistán e Iraq, además de alrededor de 150.000 cables con múltiples informaciones vinculadas a embajadas diplomáticas norteamericanas.

**06/09/ 2013**

**Revelación de *PROJECT BULLRUN*.**

El programa salió a la luz el 6 de septiembre de 2013, cuando los periodistas James Ball, Julian Borger y Glenn Greenwald publicaron en *The Guardian* las cooperaciones en clave de inteligencia entre los servicios de Estados Unidos y Reino Unido bajo el titular: *"Revealed: how US and UK spy agencies defeat Internet privacy and security"*. En el artículo se incide en que los archivos facilitados por Snowden demuestran cómo el Gobierno norteamericano ha desarrollado una tecnología capaz de des-encriptar cualquier tipo de información confidencial de los usuarios en la red, desde registros médicos a banca en línea.

**26/11/ 2013**

**Tercer Comité de la Asamblea General de la ONU, especializado en materia de asuntos humanitarios.**

Impulsó una Resolución específica sobre el derecho a la privacidad. Aunque los grandes patrocinadores de la Resolución fueron Brasil y Alemania, cuyos Gobiernos y empresas transnacionales eran de las más circunscritas a la vigilancia de la *NSA*, un total de 55 países, incluidos Francia o Rusia, apoyaron la Resolución.

**17/01/ 2014**

**Discurso de Obama sobre las prácticas de vigilancia de la *NSA* reveladas.**

La necesidad de hacer frente a las acusaciones apremió al Presidente a la comparecencia pública donde hizo balance del Estado de vigilancia y asumió su cambio de conciencia con relación a su discurso de campaña electoral. Concibiendo que en el afán de responder a las posibles amenazas globales, el riesgo de extralimitación del Gobierno y por ende, la posibilidad de privación de libertades aumentaba, Obama quiso recuperar su pensamiento crítico con la inteligencia antes de llegar a la Casa Blanca, denotándolo de *"sano escepticismo"* hacia los programas de vigilancia.

**21/02/ 2014**

**El Parlamento Europeo: Comisión de Libertades Civiles, Justicia y Asuntos de Interior.**

Redacción de un Informe titulado: *"sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior"*. A pesar de comenzar el documento admitiendo como vital, la necesaria cooperación en materia de lucha contra el terrorismo entre los Estados Unidos y la Unión Europea y sus Estados miembros, alerta de las amenazas a la intimidad en la era digital y a unas fronteras cada vez más difusas entre las actividades policiales y de inteligencia, lo cual conlleva que todos los ciudadanos sean tratados como sospechosos y estén sometidos a vigilancia.

**27/02/ 2014**

**Revelación de *OPTIC NERVE*.**

La demostración de hasta qué punto actúa el *GCHQ* en ese escrutinio salió a la luz el 27 de febrero de 2014, momento en que los periodistas Spencer Ackerman y James Ball hicieron público en *The Guardian* la existencia de una red de vigilancia clandestina, con el apoyo de la *NSA* y una activa participación del *GCHQ*, consistente en el almacenamiento de millones de imágenes de usuarios por medio del pinchazo en red, de las webcams de sus ordenadores. El programa respondía al nombre de *OPTIC NERVE*, uno de los programas de inteligencia pioneros en emplear tecnología biométrica. Tan sólo en 2008, durante un período de seis meses, la Agencia recogió un material en bruto de imagen derivado de las cámaras web, cercano a los 1,8 millones de cuentas de usuario únicas de *Yahoo!*, a nivel mundial.

**30/06/ 2014**

**La Alta Comisión de Derechos Humanos de las Naciones Unidas, ahonda en el conflicto al formular 2014 el primer informe sobre "*el derecho a la privacidad en la era digital*".**

En el mismo, la Comisión aduce a la necesidad de la vigilancia gubernamental al entender que *"los Gobiernos con frecuencia justifican los programas de vigilancia por motivos de seguridad nacional, incluyendo los riesgos planteados por el terrorismo. Varias contribuciones sugieren que, dado que las comunicaciones digitales pueden ser, y han sido, utilizadas por los objetivos criminales (para tareas como el reclutamiento o la financiación de actos terroristas), la vigilancia de la comunicación digital, puede constituir una medida necesaria y eficaz de inteligencia, siempre y cuando se lleve a cabo en cumplimiento de la legislación nacional e internacional"*.

**01/08/ 2014**

**Prórroga del derecho de asilo a Snowden en Moscú, por tres años más.**

**18/11/ 2014**

**Fracasa en la votación la reforma de la Comunidad de Inteligencia y excesos de la *NSA*. Primer intento para la *USA FREEDOM ACT.***

A pesar del gran apoyo demócrata a la Ley, con 54 votos a favor, a los que se adhirieron 4 republicanos, al no lograr reunir los 60 votos necesarios y con la oposición de 42 votos en contra, entre los cuáles 41 procedían del ala republicana de la cámara, la reforma no salió adelante.

**10/02/ 2015**

**Resolución aprobada por la Asamblea General de Naciones Unidas.**

La Asamblea distingue, en una nueva Resolución, entre las prácticas ilícitas y aquellos objetivos legítimos a los que aludía la Comisión, además de incentivar a los Estados a que *"examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad"*.

**24/03/ 2015**

**Asamblea General de Naciones Unidas. Consejo de Derechos Humanos. El derecho a la privacidad en la era digital. 28º período de sesiones.**

Señala que *"algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona, poniendo de relieve que los Estados deben respetar las obligaciones internacionales de derechos humanos en lo referente al derecho a la privacidad cuando intercepten las comunicaciones digitales de las personas"*.

**22/05/ 2015**

**Segundo intento fallido de la *USA FREEDOM ACT.***

57 a favor por 42 en contra.

**31/05/ 2015**

**Se aprueba la *USA FREEDOM ACT.***

Con 77 votos a favor y 17 en contra, el Senado confería luz verde a la nueva Ley, que automáticamente, un día antes de expirar la *USA PATRIOT ACT* entraría en vigor, sustituyendo las prácticas de aquélla. el Gobierno no esté firmemente requerido a dar explicaciones sobre el grueso de población investigada bajo la Sección 215 durante una década o el número oficial de individuos investigados al amparo de la Sección 702 de la enmendada Ley *FISA*, resta naturaleza de cambio y dota de continuismo a la política de vigilancia liderada por la *NSA* en la actualidad.

**01/06/ 2015**

**Expiración de la *USA PATRIOT ACT.***

29/11/
**2015**

**La *NSA* pierde la autoridad legal para recolectar los metadatos de teléfonos móviles.**

Gracias a la Sección 215 de la *USA PATRIOT ACT* de 2001, el *FBI* podía exigir "*cualquier material tangible*" que favoreciera el curso de una investigación para obtener información de inteligencia extranjera. De esta manera el *FBI* fue capaz de obtener los registros telefónicos de millones de estadounidenses de las compañías estadounidenses de telecomunicaciones y entregarlos a la *NSA*. La *USA FREEDOM ACT*, en vigor desde el 2 de junio, prohíbe a la Dirección Nacional de Inteligencia la recogida de registros de metadatos de teléfono a granel, comenzando el 29 de noviembre. El Ejecutivo podrá ahora obtener los metadatos de terminales móviles mediante petición al *Foreign Intelligence Surveillance Court* para ordenar a las compañías de telecomunicaciones la entrega de registros específicos.

24/03/
**2016**

**El *FBI* consigue descifrar el iPhone del terrorista de San Bernardino (California).**

Después del ataque terrorista del 2 de diciembre que causó 14 muertos y 21 heridos, el *FBI* requirió a la compañía *Apple* facilitar el acceso al terminal móvil del terrorista hallado en la escena del crimen, un iPhone. Se inició así un pulso entre el Gobierno y la compañía que arrancó cuando la magistrada federal Sheri Pym ordenó a mediados de febrero a *Apple* ayudar al *FBI* a acceder a los datos. *Apple* se negó a acceder a las peticiones del Gobierno, tras aducir que al hacerlo pondría en peligro la seguridad de todos los teléfonos iPhone. Pocas semanas después, gracias a la cooperación de la compañía *Cellebrite*, el *FBI* consiguió desencriptar el dispositivo.

16/05/
**2016**

**Nuevos documentos revelados por Snowden demuestran la cooperación entre el personal de la *NSA* y la *CIA* en interrogatorios en Guantánamo durante los primeros días de la "*Global War on Terror*".**

Ni el Informe del Comité de Inteligencia del Senado de 2014 sobre el programa de detenciones e interrogatorios de la *CIA* (que confirmó la existencia de dos instalaciones de la *CIA* en Guantánamo), ni el Informe del Comité de Servicios Armados del Senado de 2008, sobre el abuso de detenidos por los militares, abordaron el papel de la *NSA*. En la documentación revelada, con título: "*Can You Handle the Truth?*" se recoge la función de la *NSA* en los interrogatorios llevados a cabo por responsables de la *CIA* y el *FBI*. Su tarea sería la de ejecutar labores de "*interfaz con los interrogadores del Departamento de Defensa, la CIA y del FBI diariamente con el fin de evaluar y explotar la información procedente de los detenidos*". Los interrogatorios se convirtieron en actualidad a partir de la denuncia de agentes del *FBI* que protestaron internamente las tácticas de interrogatorio de las que fueron testigos, describiéndolas como "*técnicas de tortura*" y "*más allá de los límites de la práctica estándar del FBI*".

06/06/
**2016**

**El Senado aprueba una disposición que otorga al FBI más poder en las funciones de vigilancia.**

La disposición, insertada en la *Senate Intelligence Authorization Act*, autorizaría explícitamente al *FBI* para obtener "*registros de transacciones electrónicas de comunicación*" tanto de personas como entidades. En el pasado, en textos similares, estos "*registros de transacciones electrónicas*" incluían desde el historial de navegación, información de encabezado de correo electrónico, registros de las compras en línea o las direcciones IP de los contactos. El Departamento de Justicia ya en 2008 comunicó al *FBI* que no estaba autorizado a recibir esta información de las empresas sin orden judicial. No obstante, esta nueva disposición cambia el escenario.