EL DERECHO A LA PRIVACIDAD ESTADOUNIDENSE REFLEJADO EN LA FIGURA DE LA NATIONAL SECURITY AGENCY

Historia, base legal e intercepción en España.

Jose Luis Guerrero García
Trabajo Final de Grado
Facultad de Derecho
Josep Cañabate
Curso 2014/2015
15/05/2015

Resumen: Revelados los programas de investigación masiva de la *National Security Agency* se han detectado irregularidades respecto el cumplimiento de la legislación estadounidense, que determinan la desproporción entre seguridad y libertades. Es importante la figura de las autorizaciones que debe expedir una corte especial a la NSA para poder investigar a los ciudadanos estadounidenses y extranjeros, las cuales fueron erradicadas por el presidente Bush en una Orden Ejecutiva secreta, pero que a partir de la reforma del *Foreign Intelligence Surveillance Act*, fueron impuestas otra vez de nuevo, mas de una forma mucho más genérica: dando más tiempo para investigar y no a una sola persona, sino a un colectivo. Por tanto, se ha dado la necesidad, impuesta por la moral social, de regular las funciones de esta institución. Así, el escándalo de los programas de investigación de obtención de metadatos masiva de la NSA, han llegado a todas partes del mundo, incluido España, existiendo los suficientes indicios de que el Centro Nacional de Inteligencia ha facilitado información de los ciudadanos españoles a la NSA.

Abstract: Revealed the mass surveillance programs of the National Security Agency, some irregularities have been detected regarding the fulfillment of the United States legislation, which determines the disproportion between security and liberties. It is of importance to consider the figure of the warrants, which are issued by a special court for the NSA to investigate both American and stranger citizens, but the president Bush eradicated the warrants by a secret Executive Order. Nevertheless, with the Foreign Intelligence Surveillance Act reform, the warrants were again established but in a more generic way, it gives more time to investigations and it is possible to consider and investigate more than one person at a time. Such a regularization endures nowadays and thus it has given the need, imposed by the social morality, to regularize the functions of this institution. Thus, the scandal related to the investigation programs that were used to obtain mass information have reached all corners of the world including Spain and, therefore, giving us plenty of clues to assume that the Spanish *Centro Nacional de Inteligencia* has provided.

Palabras clave: Estados Unidos, National Security Agency (NSA), FISC, FISA, investigación masiva, Edward Snowden, Prism y autorización judicial.

Abreviaturas

· NSA: National Security Agency.

· HEW: Department of Health, Education, and Welfare.

· FISA: Foreign Intelligence Surveillance Act of 1978.

· FISC: Foreign Intelligence Surveillance Court.

· ECPA: The Electronic Communications Privacy Act.

· USA: United States of America.

· NCIS: Naval Criminal Investigative Service.

· AFSA: Armed Forces Security.

· URSS: Unión de Repúblicas Socialistas Soviéticas.

· FBI: Federal Bureau of Investigation.

· ACLU: American Civil Liberties Union.

· CNI: Centro Nacional de Inteligencia.

ÍNDICE

1. Introducción 4
1.1 La Cuarta Generación de Derechos Humanos 4
1.2 Control estatal ante las intromisiones a la intimidad 5
1.3 Objetivos 7
1.4 Fuentes 7
1.5 Metodología y estructura del trabajo 8
2. Derecho de la Privacidad Estadounidense 9
2.1 Antecedentes históricos 9
2.2 Progresión del derecho a la privacidad ante la revolución tecnológica 12
3. National Security Agency 16
3.1 Antecedentes, historia y definición 16
3.2 Base legal 24
3.3. Situación actual: la NSA después de las revelaciones de Snowden 33
4. Metodología de vigilancia de la National Security Agency 35
5. Relación de España con la National Security Agency 39
6. Conclusiones 46
7. Bibliografía 48
ANEXOS 56
ANEXO 1 56
ANEXO 2 61
ANEXO 3 64
ANEXO 4 67
ANEXO 5 69
ANEXO 6 71

1. Introducción

1.1 La Cuarta Generación de Derechos Humanos

Ante la gran proliferación de medios y mecanismos tecnológicos en nuestra sociedad, durante los últimos 20 años, se ha creado la necesidad de garantizar una serie de derechos ante posibles ataques. Es lo que se conoce como la cuarta generación de derechos humanos: a pesar de ello, algunos juristas especializados en la materia consideran que estos derechos aún no existen y son sólo una mera previsión, por tanto no se puede hablar de una nueva generación de derechos humanos en sí.[1] Para estos, son unos derechos que nacen directamente, sin necesidad de otra intervención que la del ciberespacio[2], es decir, el ciberespacio, indirectamente, mediante una red mundial por la que todos estamos conectados crea unos derechos inherentes a su uso[3]. Pero, tal y como advierten la mayoría de juristas, como Juan Pablo Pampillo, Paula López Zamora o Fanny Coudert[4], es necesario un marco normativo, por el que se garantice el uso del nuevo medio de comunicación: internet.

Ante esta necesidad de crear un marco legal que garantice la seguridad tecnológica, el Institut de Drets Humans de Catalunya instituye en 2003 un comité incorporado por una serie de profesionales (académicos, activistas, políticos y miembros de organizaciones internacionales), con la misión de crear un anteproyecto que contenga los derechos emergentes. Es en el marco del Fórum Universal de las Culturas[5] de 2004, celebrado en Barcelona, cuando se debate el texto por más de cien expertos y participan más de mil personas, pero no es hasta el siguiente Fórum

[1] Por ejemplo, Emilio Suñé Llinás expresa en varios escritos que estos derechos emergentes no deben considerarse como una nueva generación; así lo expresa en su artículo *Declaración de derechos del ciberespacio*: "En consecuencia, personalmente no llego siquiera a atisbar la cuarta generación de Derechos Humanos".

[2] Tal y como determina la Real Academia Española, el ciberespacio es el ámbito artificial creado por medios informáticos, es decir, es una realidad simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo.

[3] SUÑÉ, Emilio. *Declaración de derechos del ciberespacio*, Madrid: 6 de octubre de 2008, Pp. 1-4. http://portal.uexternado.edu.co/pdf/7_convencionesDerechoInformatico/documentacion/conferencias/Los_Derechos_Humanos_en_el_Ciberespacio.pdf Consultado en fecha 07/02/2015.

[4] Juristas dedicados al ámbito de la filosofía del derecho.

[5] El Fórum Universal de las Culturas no se creó por ninguna organización internacional, aunque posteriormente contó con el soporte de la UNESCO. En un primer momento, el alcalde de Barcelona manifestó su voluntad de crear dicho fórum, y la UNESCO, en su 29ª Conferencia General aprobó el proyecto.

Universal de las Culturas, en Monterrey, en el año 2007, donde se ratifica y surge el último texto, la llamada Declaración Universal de los Derechos Humanos Emergentes[6]: no sólo trata los derechos tecnológicos, sino que hace hincapié en otros derechos fundamentales, como es el medioambiente o la renta mínima ciudadana[7]. Por tanto, ante la necesidad de garantizar el buen uso de los medios tecnológicos se crea una declaración, la cual no tiene el suficiente alcance, debido a su naturaleza jurídica, y, por tanto, no vincula a los Estados. De esta manera, ante el ineficaz alcance de estas normas jurídicas, debe darse por válida la argumentación de los juristas que han tomado la postura en contra de una cuarta generación de derechos humanos, aún intangible jurídicamente: tan sólo es una "respuesta de la sociedad civil"[8] a los retos que la sociedad plantea.

La Declaración de Derechos Humanos Emergentes se basa, casi, exclusivamente en tres derechos tecnológicos. En primer lugar se encuentra el derecho a la protección de datos, consecuencia de la cantidad de datos que se recogen, transmiten y comparten, existiendo cierta preocupación acerca de la protección de los datos de cada individuo. También se encuentra el derecho a la libertad de expresión en el ciberespacio, ya que su concepción es distinta en internet, pues tal derecho adquiere una gran magnitud: la repercusión de lo expresado es mucho mayor, causando problemas al asegurar el derecho a la información veraz al resto de los ciudadanos. Y, por último, el derecho a la información, que ante las dificultades para configurarlo, como consecuencia del derecho a la libertad de expresión, es mucho más difícil controlar lo que cada ciudadano cuelga en la red[9].

1.2 Control estatal ante las intromisiones a la intimidad

> "Las leyes son las condiciones con que hombres independientes y aislados se unieron en sociedad, fatigados de vivir en un continuo estado guerra y de gozar una libertad convertida en inútil por la incertidumbre de conservarla. Sacrificaron una parte de ella para gozar la restante con seguridad y tranquilidad. La suma de todas estas porciones de libertad sacrificadas al bien de cada uno

[6] PAREJA, Estel·la. *La carta de derechos humanos emergentes: una respuesta de la sociedad civil a los retos del siglo XXI*, Barcelona: Proyecto de la Carta de Derechos Humanos Emergentes en el Institut de Drets Humans de Catalunya, 2007, Pp. 15-17.
[7] Artículo 1 y 3, entre otros, de la Declaración Universal de los Derechos Humanos Emergentes.
[8] PAREJA, Estel·la. *La carta de derechos humanos emergentes. Op. Cit.* Pp. 4.
[9] Artículos 5.8 y 5.9 de la Declaración Universal de los Derechos Humanos Emergentes.

> constituye la soberanía de la nación, y el soberano es el legítimo depositario y administrador de ellas." (…) "Fue, pues, la necesidad la que constriñó a los hombres a ceder parte de la propia libertad: es, pues, cierto que cada uno no quiere poner de ella en el depósito público más que la mínima porción posible, la que baste para inducir a los demás a defenderlo. La agregación de estas mínimas porciones posibles constituye el derecho de pensar; todo lo demás es abuso y no justicia; es hecho, no ya derecho"[10].

En este fragmento del conocido texto *De los Delitos y de las Penas* de Beccaria, el filósofo expresa, por una parte, la necesidad del principio de legalidad en derecho, y por otra, más concienzudamente, la necesidad de normas y leyes para la seguridad de la sociedad. Es decir, es necesario que existan unos estándares que protejan a todos los ciudadanos de posibles confrontaciones, los cuales deben encontrarse en cuerpos legales, expresados como normas de relevancia jurídica; siempre establecidas por un poder. A pesar de que sea el poder quien cree y garantice las normas, la convicción debe nacer de la masa social en un momento determinado de la historia. En otros términos, es lo que se entiende como moral social, que no es otra cosa que un problema compartido por una sociedad en un momento histórico concreto, que lleva al ente público legislativo a crear medidas de protección sobre las consecuencias que puedan crearse, a partir de tal problema social. Por tanto, a partir del sentir común de la sociedad se crea derecho, limitando la libertad de la sociedad, pero aumentando su seguridad.

Así, a partir de la necesidad de la sociedad, consistente en la creación de un cuerpo legal que regule sus derechos tecnológicos y de protección de la información, los Estados han llevado a cabo tareas de recopilación de unos estándares mínimos, limitando su libertad pero garantizándoles una protección; por ejemplo España ha creado la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A pesar de ello, algunos Estados, como Estados Unidos, habiendo creado estos cuerpos legales, han pecado de intervencionistas por muchos detalles, incluso vulnerando los derechos de los ciudadanos, nacidos de la convicción de estos.

[10] BECCARIA, Cesare. *De los Delitos y de las Penas*, Salamanca: Alianza Editorial, 2004, Pp. 31 y 33.

A partir de aquí, este será el caso que nos ocupará este trabajo. Es decir, ante los cuerpos legales creados por los Estados para la protección de datos de los ciudadanos, ¿realmente se han respetado, o los Estados los han vulnerado, dando prevalencia a la seguridad que a las libertades? Así, tratará, en especial, del caso *Snowden* de los Estados Unidos y de la posible vinculación del Estado español, mediante el Centro Nacional de Inteligencia, a este proyecto estadounidense. A pesar de ello, antes de entrar al tema se comentarán unas cuestiones formales.

1.3 Objetivos

El tema tratado en este trabajo es de gran relevancia, debido a que la mayoría de países del mundo sufren investigaciones y espionaje por parte de Estados Unidos. Además, cabe decir que es un tema de actualidad, ya que a partir de las filtraciones de Edward Snowden se ha creado la preocupación social y, por ende, el debate de si la tarea llevada por la NSA es legal o no, y por tanto si limita las libertades, creando un balance desequilibrado entre seguridad y derechos. Así, recientemente, el Tribunal de Apelación de los Estados Unidos ha dictado sentencia por la querella presentada por varias organizaciones privadas. Por tanto, el objetivo general de este trabajo es esclarecer la progresión del Derecho de Privacidad estadounidense ante la revolución informática, y como el gobierno lo ha interpretado y aplicado para dar poder a sus instituciones de inteligencia, como es la *National Security Agency*. Respecto los objetivos específicos cabe determinar que muchos de estos son demasiado amplios, por tanto se ha dado un tratamiento sintético a la mayoría de ellos. Uno de estos consiste en establecer la legalidad, mediante la interpretación del gobierno del Derecho de la Privacidad, de las actuaciones de la *National Security Agency*, por otra parte, otro objetivo específico es el de determinar cómo en los últimos años se ha creado una repulsa social a las actividades de investigación y espionaje, gracias a unas filtraciones, y, por último, también se esclarece la cooperación entre Estados Unidos y España para llevar a cabo investigaciones en territorio español.

1.4 Fuentes

Ante la confidencialidad de este tema resulta muy difícil encontrar fuentes que describan meticulosamente lo plasmado en el trabajo, por tanto, es necesaria una

investigación de documentos filtrados, e incluso de comparación de las pocas fuentes existentes, ya que cada autor interpreta la legalidad de la institución de una forma u otra. Por tanto, se han buscado artículos doctrinales mediante base de datos como jstor.org, ssrn.com o el aplicativo de Acceso a Recursos Electrónicos de la Universidad, pero por otra parte he llevado a cabo una tarea de investigación jurídica de documentos filtrados de la página web de Edward Snowden, Wikileaks y la web nsa.gov1.info, entre otras. En adición, me he puesto en contacto con entidades, profesores y periodistas expertos en el tema, entre los que destacan Bryce C. Newell y Joseph T. Tennis, profesores de la Universidad de Washington, Alessandro Davoli, el cual pertenece a la institución de la Unión Europea Internal Policies of the Union Policy Department C, que se encarga de velar por los derechos de los ciudadanos europeos, Miguel Gallardo, el cual ha interpuesto querella en territorio español contra la NSA, la Embajada de España en los Estados Unidos, Jonathan Mayer, el cual trabaja en el Centro de Seguridad y Cooperación Internacional y, por último con la misma NSA, que aunque contestaron no aportaron suficiente información. Cabe añadir, por tanto, que una de las fuentes más importantes, desde hace varios años, es la prensa, donde Edward Snowden ha ido filtrando documentos.

1.5 Metodología y estructura del trabajo

Este trabajo sigue un transcurso no directamente relacionado con el transcurso de los acontecimientos, sino por un orden lógico para insertar progresivamente los elementos necesarios. Así, el trabajo empieza con una breve introducción de los Derechos Humanos de Cuarta Generación, es decir los nuevos derechos humanos tecnológicos, y a continuación el control estatal de estos. Entrando ya de lleno en el objetivo general planteado, se comienza por una explicación breve del Derecho de la Privacidad de los Estados Unidos, poniendo el suficiente énfasis a partir de la revolución tecnológica. A continuación, directamente relacionado con el Derecho de la Privacidad, se empieza a explicar la historia de la *National Security Agency*, y por tanto, la base legal sobre la que se ampara sus funciones. También se explica la situación actual de la institución, para consecuentemente, determinar su método de vigilancia, ya que sin las filtraciones no se podría haber conocido nunca como investiga y espía la *National Security Agency*. Y, por último, se esclarece la relación

de España con Estados Unidos, y por tanto, la relación entre el Centro Nacional de Investigación español y la institución que es objeto de este trabajo.

2. Derecho de la Privacidad Estadounidense

2.1 Antecedentes históricos

Para entender como en la actualidad existe el Derecho de la Privacidad de Estados Unidos, debe partirse desde su origen, es decir, debe hacerse un recorrido durante la historia de esta ley.

Por tanto, debe partirse del *Bill of Rights*, es decir, desde la independencia de Estados Unidos. En este momento histórico ya se temía por la privacidad de los ciudadanos, y así lo expresa William Blackstone, enumerando algunos supuestos de hecho (a pesar de no ser uno de los fundadores de Norteamérica, sus escritos influyeron a la Constitución de los Estados Unidos): "listening under walls or windows, or the eaves of a house, to hearken after discourse, an thereupon to frame slanderous and mischievous tales"[11].

Ante la necesidad de garantizar el derecho a la privacidad, en la creación de la Constitución de los Estados Unidos de América, esto se tuvo muy en cuenta; sobre todo, a raíz del intrusismo del gobierno durante la *Revolutionary War* (1775-1783), ya que se hacía uso excesivo de su poder, saqueando, robando y allanando viviendas sin motivo. Por consiguiente, debe establecerse que no consistía en garantizar ese derecho ante terceros, sino que se unía otro sujeto más, la protección ante el Estado. Así, en la Tercera Enmienda se protege la privacidad de la vivienda ante la entrada de militares a casas ajenas. Es decir, no se permite a los militares alojarse en tiempos de paz en casas ajenas, aunque en tiempo de guerra no se deja bastante claro, ya que se determina que depende de las leyes aprobadas[12]. Por tanto, si existiera una ley que lo permitiera, los soldados podrán alojarse en casa ajena, siempre y cuando los propietarios así lo permitieran. Siendo el caso de la Tercera Enmienda, un caso especial, debe examinarse la Cuarta enmienda, la cual prohíbe los allanamientos

[11] BLACKSTONE, Sir William. *Commentaries on the laws of England (1769)*, Chicago: University of Chicago Press, cop., 1979. Facsim. Of the first ed. of 1765-1769, Pp. 168.
[12] SOLOVE, Daniel J. *A Brief History of Information Privacy Law*, Washington D.C. George Washington University Law School Public Law Research, Research Paper No. 215, Pp. 5.

injustificados y el libramiento de órdenes de allanamiento sin causa probable o fundamento.

Alcanzados el siglo XIX, nacen una serie de amenazas que deben ser garantizadas mediante el derecho. Una de estas nuevas amenazas es el censo, es decir, ante el crecimiento tan rápido de la población, los gobiernos crean un censo por tal de llevar acabo un recuento de los habitantes, y a su vez sobre las enfermedades, incapacidades y finanzas, elemento que causó un gran protesta pública, ya que se consideraba que esta práctica atentaba contra su privacidad: hecho que llevó a que el Congreso decretara que publicar información adicional de los habitantes se consideraba ilegal. Por otro lado, existía también la amenaza del correo y del telégrafo. Respecto al correo, era muy fácil que los carteros o vecinos leyeran las cartas, de esta manera el Congreso creó una ley de privacidad del correo, que aún sigue vigente. Respecto las comunicaciones por telégrafo se intentaron regular en 1880, pero no se crearon leyes en los estados, hasta que la Corte Suprema de Missouri determinó la necesidad de una ley que garantizara la privacidad de las conversaciones mediante telégrafo: fue entonces cuando, más de la mitad de los estados, crearon una ley que garantizara la privacidad en las conversaciones. Pero quizá, en el siglo XIX, los avances más importantes fueron respecto el diario y la fotografía, que se garantizaron más tarde, gracias a Samuel D. Warren y Louis D. Brandeis (a partir de ahora Warren y Brandeis), los cuales publicaron un artículo, en 1890, sobre la necesidad de crear una ley que prohibiera todas las amenazas de la vida privada cuotidiana de los habitantes norteamericanos. Así, Warren y Bandeis se basaron, primero, en la necesidad de crear una ley de privacidad ante la oleada de medios de comunicación en auge, es decir, la prensa.

Durante la segunda mitad del Siglo XIX la circulación de prensa aumentó casi en un 1.000%, y se creó la prensa amarilla, es decir, aquel periodismo que atentaba contra la vida privada de las personas, dándose un gran énfasis sobre escándalos y chismes, y que por tanto era la que daba dinero. Así, como establecen Warren y Brandeis “The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as

effrontery"[13]. Por otro lado, también se hizo hincapié en la nueva tecnológica del momento: la fotografía instantánea. Este nuevo artilugio podía inmortalizar cualquier imagen, y si se hacía una fotografía de algún escándalo, los periódicos las compraban por una gran cifra de dinero. De esta manera, concluyen determinando que se necesita un *remedy* ante estas nuevas amenazas: determinan que la *Defamation law* sólo protege la información falsa, y por tanto, es necesaria una regulación que determine la información verdadera privada[14].

Fue entrado en el Siglo XX, cuando se tuvo en cuenta la conclusión de Warren y Bandeis. En 1903, en Nueva York, se estableció un estatuto referente a la invasión de la privacidad, y en 1905, la Corte Suprema de Georgia, estableció que el derecho a la intimidad, en asuntos privados, derivaba directamente del derecho natural. Así, se establecieron los *Restatements of Torts*, que dedicaban una parte a la privacidad. Uno de los temas sobre los que trata es sobre *intrusion upon seclusion*, es decir, intrusión en la intimidad: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person[15]". Otro de los temas que trata es la revelación pública de hechos privados, y determina: "One who gives publicity to a meter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public[16]". Por último, aunque se establecen más conceptos respecto la privacidad, está la apropiación: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy[17]".

Con el descubrimiento del teléfono, y la consiguiente intercepción y control de llamadas de terceros y de los Estados, se convirtió en una amenaza, por tanto, los ciudadanos norteamericanos se dispusieron a debatir al gobierno la creación de

[13] WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*, Cambridge: Harvard Law Review, Vol. 4, No. 5, 1980, Pp. 196.
[14] SOLOVE, Daniel J. *A Brief History of Information Privacy Law. Op. Cit.* Pp. 10-12.
[15] AMERICAN LAW INSTITUTE. *Restatement of torts (second).* 1987.
[16] Ibidem.
[17] Ibidem.

alguna medida para mantener su privacidad. De esta manera, el gobierno de los Estados Unidos lo único que hizo fue abordar este tema mediante la ley que garantizaba la intimidad en las comunicaciones por telégrafo, aumentando su contenido con la privacidad de comunicaciones mediante teléfono.

A partir de 1960, se garantizó mediante sentencias de la Corte Suprema la constitucionalidad del derecho a la privacidad. Primero, en el caso *Griswold vs Connecticut* se establece que la constitución, implícitamente, garantiza una zona de privacidad, que salvaguardaba la autonomía de una persona, su cuerpo y su familia. También, en el caso, Whalen vs Roe, se determina que es cierto que existe una zona de privacidad, pero lo extiende a dos tipos de interés: por una parte, la independencia de tomar importantes decisiones y, por otra, el interés individual de evitar descubrimientos de asuntos personales[18]. Esta interpretación del derecho a la intimidad, implícito en la constitución, es lo que se pasó a llamar *constitutional right to information privacy*.

2.2 Progresión del derecho a la privacidad ante la revolución tecnológica

En la década de los sesenta, con la invención de medios tecnológicos, y sobre todo, una vez fueron asequibles para la ciudadanía, comenzó la preocupación social por violaciones a la intimidad con estos nuevos medios.

Así, en 1973, el Departamento de educación, salud y bienestar de los Estados Unidos (HEW) creó un informe llamado *Records, Computers, and the Rigths of Citizens*, el cual analizaba el problema en profundidad: "An individual must increasingly give information about himself to large and relatively faceless institutions, for handing and use by strangers-unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others[19]". Mediante este informe, se establecía la necesidad de un código de buenas prácticas de la información, el cual se creó, un año después, con el nombre de *Privacy Act of*

[18] SOLOVE, Daniel J. *A Brief History of Information Privacy Law. Op. Cit.* Pp. 23-24.
[19] *U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973*). Pp. 41.

1974. Éste, se basaba en algunos de los puntos establecidos en el informe del HEW: regulaba la colección de derechos de los ciudadanos respecto al acceso a su privacidad, la cual no podía ser entrometida por el Estado y por las agencias federales, por tanto, este código no era de aplicación para el sector privado. A pesar de que en el informe del HEW se estableciera la necesidad de restringir ciertos supuestos, como por ejemplo, la limitación el uso del número de la seguridad social en el *Privacy Act of 1974*, pero finalmente no se llevó a cabo esta; los legisladores establecieron que se usaba cada vez más como un identificador estándar universal, para el control de datos por parte de las agencias. Es decir, este tipo de código sólo sirve para establecer una restricción de la privacidad de los ciudadanos, pero no ante otros ciudadanos, sino ante los órganos estatales y federales; no llevándose a cabo lo que la sociedad exigía, es decir, garantizar su privacidad ante terceros ciudadanos[20].

Explicados los elementos básicos de la regulación de privacidad estadounidense, a partir de aquí se expresarán los elementos jurídicos que establecen la seguridad sobre la privacidad, desde el punto de vista informático. Así, a partir de 1978, con la creación del *Foreign Intelligence Surveilleance*, es cuando empiezan a nacer todos estos actos, que ya no garantizan únicamente la privacidad e intimidad física, sino que se basan en una privacidad que puede ser vulnerada mediante usos técnicos. Por tanto, respecto la *Foreign Intelligence Surveillance Act of 1978* (FISA), cabe destacar que fue creada como un régimen para la vigilancia electrónica inteligente, ante estados extranjeros, siempre que Estados Unidos formara parte del conflicto. Pero, según la cuarta enmienda, se determina que no está permitida la vigilancia a terceros, sino existe una evidencia clara de que se están llevando a cabo actividades criminales. Así, bajo la FISA sólo se podía actuar, y llevar a cabo una investigación, únicamente, cuando existieran indicios claros de que un sujeto estubiese llevando a cabo una actividad criminal, la cual luego podía presentarse como prueba ante el juicio en el que fuera parte el sujeto investigado[21]. El órgano creado para emitir las autorizaciones judiciales de investigación es el *Foreign*

[20] SOLOVE, Daniel J. *A Brief History of Information Privacy Law. Op. Cit*. Pp. 25-26.
[21] SOLOVE, Daniel J., ROTENBERG, Marc, SCHWARTZ, Paul M. *Information Privacy Law*, Nueva York., Aspen Publishin Co., 2ª edición, 2006. Pp. 29-36.

Intelligence Surveillance Court (FISC),[22] del que se hablará detenidamente más adelante.

En 1986, con el auge de un nuevo medio de comunicación, como es internet, el congreso dictó *The Electronic Communications Privacy Act* (ECPA); tal y como pasó con el aumento el uso de la prensa, el telégrafo y el teléfono. Lo que se estableció en este acto fueron unos límites para la investigación por parte de las agencias federales: la restricción de comunicaciones transmitidas, en el Título I, y la restricción de búsqueda de comunicaciones almacenadas, en el Título II. Así, en su Título III, llamado *Pen Register Act*, establecía la limitación de la búsqueda de señales de teléfonos móviles[23].

Como se puede comprobar, en ninguno de los actos jurídicos creados durante las últimas décadas se ha intentado establecer un concepto por el que se determinara la privacidad electrónica, por tanto los ciudadanos se veían desprotegidos ante la posible vulneración de esta por parte de terceras personas. Únicamente se tiene en cuenta al propio Estado y a estados terceros. Ante una nueva época, a partir del 2000, que hacía de internet, de los ordenadores y del correo electrónico un uso mayor por la sociedad, a pesar de ello, los legisladores no cambiaron su punto de mira y siguieron creando leyes para la defensa de los ciudadanos, mediante la protección social, es decir, como un derecho colectivo y no como un derecho individual de cada ciudadano. Esto se ve reflejado en la historia, sobre todo, a raíz del atentado de 11 de septiembre de 2001, cuando es creado por el Congreso la *Uniting and Stenghtening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act*, más conocido como *USA Patriot Act*[24]. Este cuerpo legal lo que determinaba era un control tecnológico mayor ante una creciente actividad terrorista. Por tanto, fue muy significativo para la FISA, que veía incrementadas sus funciones. Por una parte, se vio ampliada la definición de las limitaciones de búsqueda de señales móviles y, además, se creó la facultad de

---

[22] *Administration White Paper. Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act*. August 9, 2013. http://fas.org/irp/nsa/bulk-215.pdf Consultado en fecha 18/04/2015.
[23] SOLOVE, Daniel J. *A Brief History of Information Privacy Law. Op. Cit.* Pp. 34.
[24] RUBEL, Alan. *Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy*, Madison. University of Wisconsin, 2006, Pp. 1-2.

rastrear dispositivos, mediante búsqueda de IP, para poder revisar los correos electrónicos. Por otra parte, el acto también establecía el retraso en las órdenes de registro, es decir la tardanza para que no se pudieran interceptar anticipadamente dichas autorizaciones, aumentar los tipos de datos de contactos, a partir de los proveedores de internet y de las comunicaciones entre usuarios y, sobre todo, el control respecto los correos electrónicos, por los que se podía llegar a determinar una actividad terrorista. Pero, bajo la FISA, reformada por la *USA Patriot Act*, se crearon nuevas facultades, que consistían en que las agencias llevaran a cabo un mayor intercambio de información con estados extranjeros, y se exigió la escucha itinerante de llamadas telefónicas para poder prevenir ataques terroristas[25].

Por tanto, ante el creciente miedo del Estado ante posibles ataques terroristas, y para garantizar una protección social, se crearon una serie de figuras jurídicas. Así, en 2004 el Congreso promulgó *The Intelligence Reform and Terrorism Act*, mediante la cual se determinaba la necesidad de compartir la información respecto posibles atentados terroristas entre agencias federales[26]. Lo que se intentó con este texto fue crear una cultura de promoción de la información entre instituciones, por tal de llevarse a cabo una protección más completa de todos los estadounidenses.

Por último, en diciembre de 2005 el New York Times, en una de sus publicaciones, habla sobre el secreto de Bush. Este consistía en que había autorizado, de forma secreta, a la *National Security Agency* (agencia creada por el Presidente Truman en 1952), a que se llevara a cabo un control y una vigilancia a los ciudadanos de los Estados Unidos mediante medios electrónicos, como podía ser el teléfono móvil y el correo electrónico. Así, se creó un gran debate, determinando si el Presidente había violado, o no, la FISA[27].

En conclusión, debe determinarse que en los últimos años, tal y como se ha comentado, la privacidad ha sido uno de los derechos fundamentales más importantes a proteger, establecidos, en contraposición a la tradición europea, en varias leyes, como pueden ser la *Comon Law Torts*, la *Criminal Law*, los

[25] SOLOVE, Daniel J. *Reconstructing Electronic Surveillance Law*, Washington D.C.: The George Washington Law Review. Vol. 72:1701, 30/9/2004, Pp. 1715-1718.
[26] SOLOVE, Daniel J. *Op. Cit.* Pp. 42.
[27] SOLOVE, Daniel J. *Op. Cit.* Pp. 43.

Evidentiary Privileges, la Constitución y más de veinte estatutos federales, como la FISA. Pero debe hacerse hincapié en que el progreso y el crecimiento de las leyes de privacidad estadounidenses es debido al auge de los medios tecnológicos: es necesario un mayor catálogo de derechos fundamentales que garantice la privacidad de las personas, debido a la creación de nuevos medios tecnológicos que aumenten la incertidumbre de posibles vulneraciones en un espacio intangible, es decir en un espacio que no es físico. Pero, a pesar de ello, lo que ha hecho el Congreso ha sido únicamente crear unos medios comunes para le protección de la sociedad, sin establecer un derecho individual para que a cada ciudadano se le garantice la privacidad en internet, basándose en el miedo de conductas criminales. Por tanto, todos los ciudadanos de los Estados Unidos tienen un derecho a la privacidad de sus datos electrónicos, pero que el Estado puede entrar a vigilar en cualquier momento, para la protección de la nación, tal y como el Presidente Harry S. Truman hizo con la NSA.

3. National Security Agency

3.1 Antecedentes, historia y definición

Durante la primera mitad del siglo XX, las fuerzas militares crearon un medio de comunicación entre los mandos y el ejército: la radio tecnología. Este método usaba la criptología, emitiendo mensajes mediante códigos que fueran indescriptibles por parte de los enemigos. Por tanto, se dio la necesidad de crear un cuerpo de inteligencia militar para poder interceptar y entender dichos códigos, con la finalidad anticiparse a las estrategias militares enemigas. Así, durante la Primera Guerra Mundial, Estado Unidos creó *The Black Chamber*, también denominada *The Cipher Bureau*, que se encargaba de llevar a cabo dichas funciones. Una vez finalizada la Primera Guerra Mundial se disolvió, pero a partir de la entrada de Estados Unidos en la Segunda Guerra Mundial, se restableció, con el nombre de *Signal Security Agency* y jugó un papel de recopilación de caracteres de las demás agencias de inteligencia de los enemigos muy importante[28].

[28] HOWE, George F. *The Early History of NSA*: National Security Agency, 18/09/2007. Pp. 11-12. https://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf Consultado en fecha 20/03/2015.

Una vez terminada la Segunda Guerra Mundial, las fuerzas armadas estadounidenses, y su agencia de inteligencia se reformaron, gracias al *National Security Act*, de 1947, y se creó el *Central Intelligence Agency* y el *National Security Council*, por tal de combatir las nuevas amenazas contra la seguridad de Estados Unidos. Quizá, la agencia que cobró más importancia, a partir de 1949, fue la *Armed Forces Security Agency* (AFSA), creada en el seno del Departamento de Defensa norteamericano, la cual se encargaba de organizar toda la comunicación electrónica de las agencias civiles. A pesar de ello, era muy difícil la comunicación con agencias como el FBI o el NCIS, por tanto, el Presidente Truman ordenó la investigación de dicha institución al *Brownell Comittee*[29]. Este comité, finalmente determinó la necesidad de que esta institución recibiera más poderes y responsabilidades definidas. De esta forma, el Departamento de Defensa y el Presidente Truman decidieron crear la *National Security Agency* (NSA), y disolver la AFSA, debido a su ineficacia. De esta manera, el Presidente Truman confecciona un Memorándum, por el que establece la necesidad de crear la NSA, la cual se encargaría "to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments"[30]. Así, el día 4 de noviembre de 1952, el Presidente Truman oficializó la creación de la *National Security Agency*[31], definiéndola como la organización dentro del Gobierno de los Estados Unidos, responsable de las comunicaciones y operaciones de servicios de inteligencia, para prevenir ataques terroristas del extranjero.

Una vez creada la NSA, y expresadas sus funciones, su tarea principal, a partir del año 1953, se basó en la interceptación de comunicaciones enemigas durante la

[29] *Cryptologic Almanac 50th Aniversary Series. The Creation of NSA - Part 2 of 3: The Brownell Committee.* https://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_Creation_of_NSA_Part_3.pdf Consultado en fecha 30/03/2015.

[30] *Memorandum of October 24, 1952 for the Secretary of State and the Secretary of Defense*. https://www.nsa.gov/public_info/_files/truman/truman_memo.pdf Consultado en fecha 30/03/2015.

[31] CURRAN, Rebeca. *The National Security Agency and Domestic Surveillance*, San Francisco: Harvard Model Congress, 2015 Pp. 2-3. http://harvardmodelcongress.org/sf/wp-content/uploads/2014/11/House-Intelligence-NSA-Rebecca-Curran.pdf Consultado en fecha 30/03/2015.

Guerra Fría, en concreto, en la Guerra de Vietnam[32]. Quizá, después de la descalificación de documentos en el 2005, el hecho más considerable que se conoce durante este periodo de la historia, por parte de la NSA, es el incidente del Golfo de Tonkin. En este episodio de la historia de la Guerra de Vietnam, Estados Unidos, recibe un ataque, por parte de los norvietnamitas, en uno de sus buques (*USS Maddox*) el día 2 de agosto de 1954, pero este fracasa. A pesar de ello, dos días después, volvieron a atacar no sólo a este buque, sino a otro (*USS Turner Joy*), y finalmente consiguieron ganar el combate. Por tanto, el *Signals intelligence* (SIGINT), órgano perteneciente a la NSA, que se encargaba de la inteligencia de señales, expresó en un informe el ataque de otro buque, contra los americanos, y consecuentemente, la NSA emitió informe al Congreso sobre este. Así, ante el gran ataque de las fuerzas comunistas, el Congreso creó la *Gulf of Tonkin Resolution*, permitiendo al Presidente de los Estados Unidos, Lyndon Johnson, utilizar las fuerzas armadas estadounidenses contra los comunistas vietnamitas, y llevar a cabo una misión mayor, por tal de expulsar a soviéticos y chinos del territorio, y así crear un estado democrático-capitalista[33]. Con esto, lo que se intentó es poder erradicar el comunismo en el mundo, y dar la posibilidad a la NSA, de estar más cerca de los soviéticos por tal de poder interceptar sus operaciones; a pesar de ello, no fue hasta 1979, durante la invasión de Afganistán, cuando se pudieron descifrar los códigos de la URSS. Después de todo, en el año 2000 el historiador de la NSA Robert Hanyok llegó a la conclusión final de que el ataque del día 4 de agosto de 1954 nunca ocurrió, es decir, fue una estrategia dirigida por la NSA para poder entrar en la Guerra de Vietnam y poder combatir contra el comunismo[34]: la NSA, viciada por los altos cargos, entre los que cabe determinar la figura del Presidente, adujo en su

[32] La Guerra de Vietnam surgió por el intento, soviético, de unificar Vietnam en un solo territorio comunista: por una parte, Vietnam del Sur era aliado de Estados Unidos, y por otra, la República Democrática de Vietnam (Vietnam del Norte), que era aliado de la URSS y de China. Por tanto, se considera una de las batallas más importantes de la Guerra Fría, disputada entre el bando comunista y capitalista: con gran proyección de Estados Unidos y la URSS.

[33] JOHNSON, Thomas R., *American Cryptology during the Cold War. 1945-1989: Book II: Centralization Wins 1960-1972*: National Security Agency: Center for Cryptological History, 1995, Top Secret Umbra, Pp. 515-518.

[34] HANYOK, Robert. *Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964*. Cryptologic Quarterly, Edition Winter 2000/Spring 2001, Vol. 19, No. 4 / Vol. 20, No. 1.
https://www.nsa.gov/public_info/_files/cryptologic_quarterly/Skunks.pdf Consultado en fecha 31/03/2015.

informe un ataque, que nunca había ocurrido. Este informe se confeccionó en la legislatura de Bush, y se mantuvo en secreto por tal de que la sociedad no hiciera comparaciones con la invasión de Iraq. Así, en octubre de 2005, el New York Times publicó las opiniones de Hanyok, hecho que hizo que la NSA descalificara todos los documentos relacionados con los hechos.

Por tanto, queda claro que la primera función que llevó a cabo la NSA fue la descodificación de códigos de los comunistas, en concreto, de la URSS y de China, haciendo una gran tarea, sobre todo, en la década de los sesenta, cuando se evitó la explosión de la primera arma nuclear china[35]. Pero, a partir de los atentados del once de septiembre de 2001, sus funciones han cambiado[36].

El atentado del once de septiembre de 2001, por parte de *Al Qaeda*, conmocionó a la población estadounidense, pero además la comunidad de inteligencia debatió por qué la NSA no detectó a tiempo los ataques, ya que existían evidencias. En junio de 2001, el *Federal Bureau of Investigation* (FBI) de Phoenix, publicó un memorándum, estableciendo que Osama Bin Laden tenía la intención de enviar terroristas de *Al Qaeda* en vuelos hacia Estados Unidos, para llevar a cabo un atentado. Se estableció que los terroristas eran estudiantes de las escuelas de vuelo de los Estados Unidos, y por ende, el memorándum propuso cuatro recomendaciones: la primera recomendación consistía en crear una lista de los vuelos de las escuelas de aviación, la segunda recomendación determinaba la necesidad de establecer enlaces con dichas escuelas, la tercera consistía en descubrir e investigar los planes de Bin Laden con la comunidad de inteligencia, y por último, que se creara una lista de las tarjetas de crédito de los estudiantes. A pesar de ello, ninguna de las recomendaciones fue tomada en cuenta por el FBI, ya

[35] BURR, William. *The United States, China, and the Bomb.* National Security Archive Electronic Briefing Book Nº1.
http://nsarchive.gwu.edu/NSAEBB/NSAEBB1/nsaebb1.htm Consultado en fecha 04/04/2015.
[36] *Liberty and Security in Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications*
https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf Consultado en fecha 04/04/2015.

que, realmente el memorándum de Phoenix no se leyó hasta pasado el 11 de septiembre[37].

A partir del 11 de septiembre se creó una consciencia social compartida para luchar de manera más fuerte contra el terrorismo. De esta manera, una semana después de los atentados, se creó *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, también conocido como *USA Patriot Act*, con el objetivo de ampliar el control del Estado para combatir contra el terrorismo, mejorando la comunicación entre las instituciones de seguridad y dotándolas de mayores funciones de vigilancia contra el terrorismo; además se crearon nuevos delitos y se endurecieron las penas por terrorismo, restringiendo más las libertades de los ciudadanos norteamericanos. Además, se determinó que no se iba a investigar única y exclusivamente a terceros estados, sino que a partir de la creación de esta ley, se podrían también investigar personas estadounidenses y residentes en su territorio[38]. Por tanto, se incrementó la vigilancia del Estado mediante la expansión de la capacidad del gobierno para poder comprobar los registros de los terceros, la posibilidad de poder llevar a cabo investigaciones en propiedades privadas sin autorización, la necesidad de colección de inteligencia extranjera y la disminución de las restricciones en las leyes, dando la potestad al Estado de poder realizar escuchas telefónicas. Estas dos últimas facultades se convierten en exclusivas de la NSA: anteriormente al atentado ya podían recopilar inteligencia extranjera, pero con la *USA Patriot Act* se le da la facultad de poder realizar escuchas telefónicas, con la de poder llevar a cabo investigaciones sobre terroristas[39].

Una vez establecidas estas competencias a favor de la NSA, el Presidente Bush decide, ante la amenaza terrorista, investigar, no sólo, a personas de terceros estados, sino que también autoriza a la NSA para que lleve a cabo la escucha

---

[37] HILL, Eleanor; *The FBI's Handing of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2011*. 24 de septiembre de 2002. p.p. 5. http://www.intelligence.senate.gov/021017/hillunclass.pdf Consultado en fecha 04/04/2015.

[38] STAPLES, William G. *Encyclopedia of Privacy: volume 1: A-M*. Greenwood Press, London: Greenwood Press, 2007, Pp. 349-351.

[39] SOLOVE, Daniel. *Data Mining and the Security-Liberty Debate*, Washington D.C.: George Washington University Law School, 2008. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2084&context=faculty_publications

telefónica de ciudadanos de los Estados Unidos, posiblemente relacionados con *Al Qaeda*, de forma secreta y sin ninguna autorización judicial (*intra, se explicará más adelante)*; hecho que se relata en el periódico New York Time, en el año 2005[40]. Por tanto, en un primer momento, se acusó al Presidente Bush de haber vulnerado la FISA. Inicialmente, el Presidente Bush se negó a contestar dicha acusación, pero más adelante, expresó que sí usó la NSA para interceptar llamadas telefónicas, sin ningún tipo de autorización, en el marco del *Terrorist Surveillance Program*[41], para poder interceptar dichas llamadas dentro y fuera de los Estados Unidos. Además, añadió que no era necesaria ninguna orden judicial, ya que "Congress gave me the authority to use necessary force to protect the American people, but it didn't prescribe the tactics.*"*[42] Es decir, Bush determinaba que en su persona recaían varios derechos, y uno de ellos consistía en la protección de la seguridad nacional, y él intervino con escuchas telefónicas, por tal de garantizarla: colisión de derechos, por una parte derecho a la intimidad y, por otra, derecho a ser protegido. A pesar de ello, Bush sabía que esas palabras no eran suficientes para tranquilizar a la población, por tanto hizo usos de medios jurídicos: el 10 de julio de 2008 Bush firmó la ley de enmiendas de la FISA, la cual otorgó inmunidad a las compañías de comunicación que habían participado en las escuchas telefónicas. Pero quizá lo más impactante de esta ley, y lo más importante para llegar al momento actual de la NSA, consistió en que no se requeriría, a partir de la entrada en vigor de la ley, ninguna autorización al FISC que determinara la existencia de que tal persona estaba relacionada con una banda terrorista, para poder investigar a personas ciudadanas y residentes de los Estados Unidos. De esta manera, la FISC, se encargaba de crear autorizaciones judiciales para colectivos de personas y terceros estados: con la entrada en vigor de esta ley, la NSA solo debe presentar unas cuestiones que consecuentemente serán aprobadas por la FISC, dando autorizaciones judiciales de investigación de forma muy genérica. Esta ley la usó

[40] http://www.nytimes.com/2005/12/18/politics/18bush.html?pagewanted=all&_r=0 Consultado en fecha 08/04/2015.

[41] Es parte del *President's Surveillance Program*, la cual autoriza al gobierno a llevar a cabo escuchas telefónicas, sin ningún tipo de autorización judicial, de las comunicaciones internacionales, cuando se tenga la certeza de que cierta persona es parte de una célula terrorista, que tenga por objetiva atentar en territorio estadounidense.

[42] LEE, Newton. *Counterterrorism and Cybersecurity: Total Information Awareness*, New York: Editorial Springer, 2013. Pp. 54.

Bush para salir del paso, queda claro cuando se determina en la misma que tenía un periodo de vigencia determinado, pero a pesar de ello, se han ido renovando después de cada periodo de vigencia[43].

Por tanto, las funciones y facultades de la NSA han cambiado a lo largo del tiempo, por tanto también ha cambiado su definición: "NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes" […] "is considered to be America's code-breaking organization, established to protect the United States from threats to national security[44]". Se puede determinar fácilmente que esta es una definición general e incompleta, pero ante la incerteza y secretismo que marcan a esta institución, no queda más remedio que compilar una propia definición de esta. Analizados varios elementos, esta podría ser una definición de la NSA del momento actual: Es una institución civil y militar especializada en criptología,[45] estructurada en dos divisiones: por una parte el *Signals Intelligence* y, por otra parte, la *Information Assurance*, cuyo objetivo principal es espiar a estados terceros, organizaciones y personas, no sólo extranjeras, e incluso a líderes políticos y militares. Por tanto, la función y misión principal de la NSA es el espionaje para preservar la seguridad nacional, en materia de terrorismo. Debe esclarecerse la gran influencia militar que recibe esta institución, ya que depende del Departamento de Defensa, y el director es un oficial de tres estrellas del ejército. Así, debido al poder de los Estados Unidos en el marco internacional, y al miedo causado por los atentados, y la consecuente obsesión por proteger el territorio, la influencia, tanto política como militar, es patente en esta institución, hecho que se ha llevado al debate internacional. Por ende, es una institución que ha vulnerado el derecho a la intimidad y privacidad a casi todo ciudadano del mundo, por tal de preservar su seguridad nacional; hecho que destapa una gran desarmonización, por la que se han vulnerado derechos de personas no residentes, ni ciudadanos de los Estados Unidos,

[43] GAINER, Randy. *The NSA's interception of emails and phone calls in the US is unlawful*, Cleveland: Journal of Internet Law, Vol.9 Nº 8, Feb. 2006, Aspen Publishers, Inc.
[44] *NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes*. 9 de agosto de 2013. https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf Consultado en fecha 15/04/2015.
[45] La criptología es la ciencia que se encarga de codificar y descodificar información.

sin la posibilidad de garantizarle a estos un cierto margen de protección. Es decir, lo que intenta el gobierno, con la NSA, es garantizar la protección a todos los ciudadanos de los Estados Unidos, pero dentro de su plan se encuentra la necesidad de investigar a personas no residentes ni ciudadanas de los Estados Unidos, que ven vulnerado su derecho a la intimidad sin poder recibir una protección antiterrorista. De esta manera, puede determinarse que el panorama internacional está bajo las órdenes de los Estados Unidos, ya que la mayoría de estados democráticos, aun viendo que se les está vulnerando, no sólo a sus ciudadanos, sino a sus líderes también, el derecho a la intimidad, han decidido cooperar con la institución, llevando a cabo investigaciones en los propios territorios, con la finalidad de enviárselo a la NSA (supra). Otra cuestión muy importante para confeccionar la definición de NSA es la de los escándalos llevados a cabo por ésta, viéndose obligados incluso, en 2005, a crear un plan de transparencia por el que se descatalogaron y salieron a la luz varios documentos, para esclarecer ciertos actos llevados a cabo: uno de los más significantes es el del Golfo de Tonkin, comentado anteriormente. Por último, debe hacerse hincapié en la confidencialidad: los métodos de la NSA están fuertemente encriptados. Este hecho hace que cree más incertidumbre entre la ciudadanía; a pesar de ello, es necesario para evitar que los terroristas conozcan sus estrategias y planes. Pero, un hecho que ha marcado la historia de la NSA han sido las revelaciones de Edward Snowden, trabajador contratista de la institución: a pesar de la fuerte codificación y el secretismo, Snowden ha decidido destapar las estrategias de la NSA, ya que las consideraba abusivas. A partir de las declaraciones de Snowden, se llega a la conclusión de que la definición de NSA cambia más aún. Por tanto, se puede determinar que la NSA es una institución dependiente del Departamento de Defensa de los Estados Unidos, que se encarga, a través de la NSA, a investigar, ya no sólo para conocer los posibles terroristas, sino que se lleva a cabo una investigación y un almacenamiento de datos masivos para conocer distintos datos de los habitantes del mundo. Así, esta institución lleva a cabo un uso arbitrario de sus competencias, no restringiéndolas únicamente a recoger datos para que prevalezca la seguridad nacional, sino que los datos recogidos pueden llegar a recoger información no relacionada con el terrorismo, simplemente para determinar los intereses de la sociedad.

3.2 Base legal

Así, se llega a la determinación de que la *National Security Agency* fue creada para la investigación de posibles actos terroristas en el territorio estadounidense, y en consecuencia, para la paliación de estos. Por tanto, es necesaria una base legal que permita a dicha institución llevar a cabo sus funciones, la cual será objeto de estudio en este apartado.

Primero debe dejarse claro que el objeto de la *National Security Agency*, tal y como se ha explicado anteriormente, ha cambiado en el paso de los años. Así, en el momento de su creación se quería hacer uso de ella solamente para investigar a los ciudadanos, organizaciones y gobiernos extranjeros, es decir, su función principal consistía en llevar a cabo investigación, sobre todo, de las fuerzas comunistas para velar por la protección nacional.

De esta manera, en 1978 se promulgó el *Foreign Intelligence Surveillance Act of 1978* (FISA), el cuerpo legal necesario para que la NSA pudiera cumplir con sus funciones. Así, la FISA, es la figura jurídica que se encarga de regular la vigilancia de inteligencia extranjera: función principal de la *National Security Agency*. Por tanto, en este momento, creada la institución y la ley, Estados Unidos recibe la plena potestad para investigar a sujetos extranjeros, por medios telefónicos y a través de internet, sin la autorización pertinente de ningún estado, ni aliado ni enemigo (sección 702 FISA). Por tanto, se entiende la supremacía de Estados Unidos en el panorama internacional, ya que ningún estado, en un primer momento, se opone a una investigación por parte de Estados Unidos; muchos autores hablan de un Big Brother[46], que vela por la protección internacional, y por tanto, restringiendo las libertades inherentes a sus ciudadanos y ampliando la vigilancia, ya no por parte del estado al que pertenecen, sino por un tercero estado.

Al paso del tiempo, las necesidades se fueron haciendo mayores, y por tanto, ya no sólo se investigaba a ciudadanos extranjeros, sino que se pretendía espiar también a ciudadanos de los Estados Unidos; por considerarse personas afectas al régimen

[46] SOLOVE, Daniel J. *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, Stanford: Stanford Law Review, George Washington University Law School, julio del 2010.

de *Al Qaeda*, o simplemente por considerarse que sus actos estaban estrechamente relacionados con el terrorismo y, por tanto, podían suponer una amenaza de la protección nacional. Así, la FISA crea un mecanismo por el que es posible la investigación de ciudadanos norteamericanos, siempre y cuando, una corte especial diera la orden judicial pertinente. Esta corte especial, es la llamada *United States Foreign Intelligence Surveillance Court* (FISC), creada por la FISA. La posibilidad de investigar a ciudadanos estadounidenses era cada vez más palpable, así, el gobierno hizo uso de esta potestad concedida por el ordenamiento jurídico, e investigó a sus ciudadanos.

La FISA da la posibilidad de investigar a los estadounidenses, pero sólo a un sujeto, que no es otro que el gobierno federal, ya que tal y como establece el texto constitucional, el único encargado de velar por la protección nacional es el presidente.[47] Así, el gobierno de los Estados Unidos empieza a hacer uso de dicho trámite, el cual consiste solamente en presentar recursos ante la FISC, para que los apruebe o no. Debe tenerse en cuenta que la FISC es creado como un tribunal súper secreto, debido a la información que recoge; se han descodificado muy pocas sentencias de este tribunal, y solamente en parte.

En consecuencia, se puede determinar que este trámite procedimental es una acción de llover sobre mojado, ya que un ente, como es la FISC, creada por la FISA, que a la vez es promulgada por el gobierno, va a resolver favorablemente la investigación sobre ciudadanos estadounidenses (existen muy pocos casos que se han denegado, ya que se han usado para que la sociedad no entendiera la arbitrariedad de dicho tribunal), ya que conservar la protección nacional es una tarea compartida.

El trámite es bastante sencillo. Primero, en el caso de que el gobierno de los Estados Unidos quiera investigar a un ciudadano concreto, debe presentar una orden de vigilancia, llamadas ordenes FISA, lo suficientemente motivada, ante un juez individual de la FISC. A partir de ese momento se habla de un proceso unipersonal,

[47] Del deber del presidente de garantizar la seguridad nacional, recogido en el artículo II de la Constitución de Estados Unidos, emana lo que se denomina "privilegio ejecutivo". Este consiste en que, en el caso que haya un escándalo, el Presidente puede codificar la información por tal de preservar la seguridad nacional.

ya que, al tratarse de casos secretos, la parte a la que se pretende investigar no puede estar presente; además las audiencias son cerradas al público. A partir de ese momento el juez debe determinar si es necesario llevar a cabo dicha investigación, y, lo que más tiene en cuenta, es si existe un motivo razonable para llevarla a cabo. Dicho motivo razonable está íntimamente relacionado con la protección nacional, es decir, cuando se conozca una causa probable de que dicha persona va a llevar a cabo actividades terroristas. Finalmente, en el caso que el juez de la FISC considere necesaria la investigación de un ciudadano de los Estados Unidos, dictará sentencia a favor, y dará vía libre a la *National Security Agency* para que investigue sus llamadas telefónicas, emails, faxes… Por tanto, la tarea que lleva a cabo la FISC, es considerar si dicha investigación cumple los requisitos legales, es decir, si cumple la FISA[48].

Establecida una orden de investigación bastante omnicomprensivo, en el que era posible la investigación a extranjeros y a ciudadanos, siempre que la FISC otorgara autorización judicial, el 11 de septiembre de 2001 cambió todo. Con los atentados, la seguridad nacional y, por ende, las investigaciones y espionaje de personas relacionadas con el terrorismo aumentó considerablemente. Ante la obsesión del gobierno federal ante el terrorismo, George Bush, tal y como se ha explicado anteriormente, creó una orden ejecutiva[49], con la que determinaba como necesario y urgente que la NSA pudiera espiar a los ciudadanos de los Estados Unidos sin ningún tipo de orden judicial[50]. De esta manera, George Bush, de forma secreta, determina que es posible la actuación de la NSA, aunque no existe indicio razonable de que un ciudadano pertenezca a una célula terrorista. Las consecuencias de esta

[48] *Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act. Op. Cit.*

[49] Las órdenes ejecutivas son documentos por los que el Presidente de los Estados Unidos puede gestionar las operaciones del gobierno federal.

[50] Hecho que vulneró completamente la FISA y la jurisprudencia de la Corte Suprema. La Sentencia United States v. U.S. District Court. 40, U.S. 297 (1972), también conocida como caso Keith, es una de las sentencias más conocidas respecto la necesidad de las autorizaciones judiciales. En este caso se determina que el gobierno de los Estados Unidos no tiene autoridad inherente para investigar y espiar sin orden judicial a los estadounidenses. Esta decisión fue aprobada por la Corte Suprema por unanimidad el 19 de junio de 1972. Sin embargo, el poder ejecutivo argumentó que el presidente mantiene el poder constitucional para autorizar la vigilancia electrónica sin la autorización judicial pertinente, ya que es el encargado de la seguridad nacional. Este debate se llevó al Congreso, y finalmente se aprobó la FISA en 1978, la cual determina que es necesaria la orden judicial para vigilar y espiar a estadounidenses en el extranjero, las cuales deben ser expedidas por la FISC.

orden ejecutiva es la llamada *Domestic Surveillance* (*NSA warrantless surveillance*)[51], es decir, la investigación de ciudadanos estadounidenses, sin la autorización judicial de la FISC. Por tanto, se puede determinar que dicha orden ejecutiva vulneraba la FISA, ya que era necesaria la intervención de la FISC, a pesar de ello, George Bush alegó que el texto constitucional insistía en que el Presidente de Estados Unidos tiene la potestad de crear cualquier mecanismo para la prevención de la seguridad nacional[52], y que esto era necesario, después del ataque del 11 de septiembre. A pesar de ello, para que no hubiera lugar a dudas, en 2008, tres años después de que se descubriera esto, la Administración de Bush creó una reforma de la FISA, la cual enmendaba alguno de sus artículos. Los dos puntos más importantes respecto esta reforma fueron la inmunidad que recibieron las empresas que ayudaron al gobierno a llevar a cabo el espionaje de estadounidenses, y la instauración de la autorización judicial de la FISC para poder investigar. A pesar de ello, Snowden ha declarado en sus entrevistas, que la NSA ha interpretado la ley a su manera: sí se piden las autorizaciones judiciales, pero estas duran de 90 días y son muy genéricas, es decir, se da la capacidad de investigar a cualquiera estadounidense[53]. Por tanto, de una investigación muy reducida, se pasa a una investigación masiva de todos los estadounidenses, sin ningún filtro ni restricción. Todo y eso, el Director de Inteligencia Nacional emitió comunicado expresando que eso era falso[54]. Esta ley de enmiendas se creó para un período de cinco años (vigente hasta el 1 de junio de 2015), a pesar de ello, se ha vuelto a aprobar de nuevo.

Pero a partir de qué presupuesto puede investigar el gobierno de Estados Unidos puede investigar a ciudadanos estadounidenses, qué precepto legal lo ampara, ya

---

[51] WONG, Katherine. *The NSA Terrorist Surveillance Program*, Cambridge: Harvard Journal on Legislation, Vol. 43, No. 2, 2006, Pp. 517.

[52] Artículo II de la Constitución de los Estados Unidos.

[53] ROLLINS, John. *NSA Surveillance Leaks: Background and Issues for Congress*: Congressional Research Service, 4 de septiembre de 2013, Pp. 10-11. https://www.fas.org/sgp/crs/intel/R43134.pdf Consultado en fecha 20/04/2015.

[54] Office of the Director of National. *ODNI Statement on the Limits of Surveillance Activities Intelligence*. Washington, DC. 16 de junio de 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/880-odni-statement-on-the-limits-of-surveillance-activities?tmpl=component&format=pdf Consultado en fecha 20/04/2015

que tal y como establece la cuarta enmienda de la constitución es inviolable la esfera personal de los ciudadanos.

Después de los ataques a las torres gemelas, se promulgó lo que se conoce como la *USA Patriot Act*, la cual ampliaba las capacidades del gobierno y de las agencias federales para combatir el terrorismo. Así, una de las leyes sobre la que enmendó más fue la FISA, introduciendo ciertos aspectos por tal de que el gobierno y, por ende, la NSA, pudieran llevar a cabo sus funciones de forma más flexible: sobre todo deben tenerse en cuenta las secciones 702 de la FISA, y, en especial trascendencia, la secciones 215 y 206 de la *USA Patriot Act*: ley que estará vigente hasta el día 1 de junio de 2015.

Así, la sección 215 de la *USA Patriot Act* (la cual reforma la sección 501 de la FISA) autoriza al gobierno a obtener cualquier cosa tangible, de un estadounidense, siempre que sea relevante para una investigación terrorista, aunque no existan indicios de que dicha cosa tangible se refiera a células terroristas, presuntos terroristas o actividades terroristas. Por tanto, se debe determinar que esta sección faculta a interceptar "any tangible things including books, records, papers, documents, and other ítems[55]". En base a esta sección, el gobierno de la NSA se escuda en que los datos de internet y las llamadas telefónicas son objetos tangibles, y por tanto, pueden ser objeto de una investigación terrorista. Interpretando de forma extensiva el texto, se autoriza a la NSA a crear una base de datos donde se recojan los objetos tangibles de ciudadanos extranjeros e, incluso, estadounidenses[56]. Dentro de esta sección se determina que el gobierno tiene la potestad a acceder a negocios privados, tanto de ciudadanos, como de empresas privadas, siempre que sea identificable una causa probable de conexión[57]. Cabe decir, que para llevar a cabo la recopilación de una base de datos de escuchas telefónicas, mediante esta sección, se obliga también implícitamente, a las empresas

[55] Section 501 FISA. Access to certain business records for foreign intelligence and international terrorism investigations.
[56] SHANE, Peter. M. *Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance,* Ohio. Journal of Law and Policy for the Information Society, No. 228, November 25, 2013.
[57] ROLLINS, John. *NSA Surveillance Leaks: Background and Issues for Congress. Op. Cit.* Pp. 4-8.

de comunicación estadounidenses a cooperar para dicho fin[58]. Por tanto, de una forma explícita, no se entiende de dicho artículo esta posibilidad, a pesar de ello, el gobierno ha considerado que la sección 215 debe garantizar la función de la NSA, por la que, entendida de forma amplia, tiene libertad para investigar a cualquier persona, ya que no es exigible que exista sospecha, y, además, no se restringe a un tipo de cosas tangibles, por tanto, casi cualquier cosa puede encontrarse dentro de esta calificación.

Por su parte, la sección 206 de la *USA Patriot Act*, también llamada *roving John Doe wiretap*, extiende a la NSA la capacidad de seguir un objetivo, en vez de vigilar los medios o las instalaciones, siempre que las acciones de medios e instalaciones puedan frustrar la vigilancia. Es decir, lo que permite la sección 206 es flexibilizar la forma en que se investiga a las personas, ya que no es obligatorio investigar el medio (por ejemplo, el teléfono u ordenador, que también se puede hacer), sino que es más efectivo investigar directamente a la persona[59]. Por tanto, aunque varias leyes expresen que la NSA sólo recopila los datos superfluos, como son la duración de la llamada, o el destinatario de esta, esta sección, da la posibilidad de poder escuchar en sí la conversación telefónica, es decir, el objeto de la investigación.

Respecto otras exigencias de la FISA, también debe tenerse en cuenta la sección 702 de la FISA, la cual determina, por una parte que es posible la investigación, con la autorización judicial concreta, a estados extranjeros, sus organizaciones, ciudadanos o jefes políticos, y por otra, se determina que ningún ciudadano estadounidense puede ser intencionadamente investigado, a excepción de que existan indicios de que puede ser un presunto terrorista, o que pertenece a una célula terrorista[60]. Por tanto, entendiendo esta sección de forma amplia, se llega a la conclusión de que cualquier estadounidense puede ser investigado por la NSA, ya que al no poderse investigar a ningún estadounidense de forma premeditada, se hace

[58] RUBEL, Alan. *Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy*. *Op. Cit.* Pp. 125-128.
[59] DOYLE, Charles. *Terrorism: Section by Section Analysis of the USA PATRIOT Act.* "Section 206. Roving Surveillance Authority under the Foreign Intelligence Surveillance Act of 1978". 10 de diciembre del 2001.
https://epic.org/privacy/terrorism/usapatriot/RL31200.pdf Consultado en fecha 23/04/2015.
[60] YOO, John. *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, Berkeley: UC Berkeley Public Law Research Paper No. 2369192, 1 de diciembre del 2013, Pp. 9-11.

uso de un método aleatorio para no investigar a ningún ciudadano deliberadamente. Al expresarse que cualquier persona puede ser investigada por la NSA, aunque no sea intencionadamente, lo más probable es que se haya investigado, al menos una vez, a todos los estadounidenses[61]. Adicionalmente, cabe determinar que esta sección es la que expresa los tipos de autorizaciones judiciales que debe pedir la NSA para investigar. Respecto las personas extranjeras, se determina que no debe pedirse ningún tipo de orden judicial, pero que para ciudadanos estadounidenses, que se encuentren dentro del territorio nacional, debe pedirse autorización judicial, y para ciudadanos que no se encuentren dentro del territorio nacional, debe pedirse una orden combinada.

Pero ni la FISA ni la *USA Patriot Act* recogen todos los presupuestos, debe tenerse en cuenta así, la orden ejecutiva 12333. Esta orden ejecutiva determina la posibilidad a los Estados Unidos de "collects, retains, analyzes, and disseminates foreign signals intelligence information[62]". Es decir, da la potestad al gobierno de poder investigar a estados terceros, cosa que no expresa la FISA. Por tanto, puede reunir información de inteligencia extranjera de los sistemas de comunicación de alrededor de todo el mundo. A pesar de ello, interpretando implícitamente dicho texto, el gobierno tiene la potestad de investigar a ciudadanos estadounidenses, siempre y cuando un extranjero se comunique con este. Es decir, cuando se sepa que un extranjero es terrorista y se comunique con alguna persona estadounidense, este texto legal da la potestad al gobierno de poder investigarlo. Cabe determinar, que esta es la figura legal que hace que el gobierno de los Estados Unidos puede investigar a todos los ciudadanos estadounidenses, ya que, según sus métodos de investigación puede entenderse relacionado con un terrorista: por ejemplo, cuando las ondas del teléfono móvil de un ciudadano estén cerca de las de un terrorista[63]. Pero debe tenerse en cuenta su artículo 2.3, por el que se establece que el gobierno

[61] DONOHUE, Laura K. *Section 702 and the collection of international telephone and internet content*, Cambridge: Harvard Journal of Law & Public Policy, Winter 2015, Pp. 104.
[62] National Security Agency. The National Security Agency: Missions, Authorities, Oversight and Partnerships, 9 de agosto de 2013.
https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf
Consultado en fecha 01/05/2015.
[63] *Liberty and Security in Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Op. Cit.*

solo podrá investigar a una persona estadounidense, si lo permite la legislación aplicable, si la información se ajusta a un de las categorías enumeradas en dicha orden ejecutiva y si lo permiten las directrices de aplicación de las agencias de inteligencia; hecho que podría devastar las investigaciones a ciudadanos de los Estados Unidos, llevadas a cabo por una probabilidad de cercanía con una célula terrorista, sin tener la suficiente motivación para espiarlo.

Además, cabe determinar el cometido, es decir, las funciones que debe cumplir la *National Security Agency*, están recogidas en el artículo 1.12 b) de la orden ejecutiva 12333, pero la misión principal es la seguridad nacional, entendida desde un punto de vista colectivo, es decir, restringir la privacidad personal individual y garantizar la seguridad nacional colectiva. En el presente caso, se puede llegar a entender que incluso la privacidad personal se ha restringido totalmente, ya que, los ciudadanos estadounidenses pueden ser investigados por el gobierno, por tal de la protección de un bien jurídico indeterminado, es decir, la protección de la seguridad nacional no se puede entender como algo determinado, y menos como algo dirigido a individuos concretos, simplemente se entiende como un algo generalizado para todas la población. Por otro lado, lo que intenta la NSA es reducir riesgos, ya que si se tienen controlados los terroristas es fácil una interceptación de estos. También, otra de sus funciones es el esclarecimiento de la verdad, respecto los estados extranjeros, ya que algunos estados están, por ejemplo, muy influenciados por la religión, y sobre todo, religiones como la musulmana puede tener extremistas que pueden llegar a inmolarse, tal y como pasó el 11 de septiembre de 2001[64].

Finalmente, debe hacerse hincapié en el debate jurídico respecto si George Bush vulneró la FISA, y si realmente la NSA cumple con las exigencias de la cuarta enmienda de la constitución de los Estados Unidos. Respecto el primer tema, debe llevarse a cabo una ponderación, por la que se determine si realmente es necesaria la autorización judicial, por parte de una corte especial, para poder investigar a los ciudadanos estadounidenses. Cabe decir que aquí entran en colisión dos poderes, por una parte el ejecutivo, y por otra el judicial y legislativo; se unifican judicial y legislativo, ya que la jurisprudencia, dentro del sistema jurídico norteamericano, es

[64] *Liberty and Security in Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Op. Cit.*

considerada una fuente de derecho. Por una parte, el poder ejecutivo, representado por el Presidente de los Estados Unidos, en este caso George Bush, aduce que el artículo II de la Constitución le da el poder inherente para velar por la protección nacional, y que por tanto, es legal dar la potestad a la NSA para investigar a ciudadanos estadounidenses sin la autorización judicial de la FISC, pero por otra parte, la FISA expresa la necesidad de que el gobierno, en el caso de que quiera investigar a ciudadanos norteamericanos, es necesaria una autorización judicial por parte de la FISC. Incluso en sentencias, como la que se ha comentado anteriormente (United States v. U.S. District Court. 40, U.S. 297 de 1972), la Corte Suprema se ha ratificado determinando que es obligatoria una autorización judicial. Por tanto, en este punto cabe determinarse cuál es la posición correcta, y por ende, determinar que tiene más relevancia una orden ejecutiva o una ley. Así, basándonos en teorías de purificación del derecho, como es la pirámide de Kelsen, debe determinarse que George Bush vulneró la FISA, ya que las leyes tienen un estatus más alto que las órdenes ejecutivas, pero desde un punto de vista proteccionista, puede llegarse a determinarse que, a pesar de que George Bush vulnerara la FISA, al otorgarle la Constitución la protección nacional, actuó de forma lógica ante la vulneración de esta, en los atentados del 11 de septiembre. Desde un punto de vista subjetivo, considero que el derecho es una ciencia pura, y que por tanto la actuación de Bush no fue la correcta, ya que vulneró un cuerpo legal y, en consecuencia, restringió los derechos que la FISA recoge a los ciudadanos de los Estados Unidos, a pesar de que se hubiera atentado contra la protección nacional. Respecto la constitucionalidad de la NSA, debe determinarse que no se puede examinar como una unidad, ya que es necesario conocer los programas y la metodología de vigilancia de esta institución, por tanto, se considera que este trabajo no examinará la constitucionalidad de cada programa de vigilancia, ya que se excedería. Así, en los siguientes apartados se estudiará la situación actual de la NSA, haciéndose hincapié en las declaraciones del Caso Snowden, ya que gracias a este se han descubierto todos los programas de vigilancia de la NSA. De esta manera, primero se explicará la situación actual de la NSA y, de manera consecuente, los programas de vigilancia utilizados por esta.

3.3. Situación actual: la NSA después de las revelaciones de Snowden

La situación actual de la NSA quizá es la época más compleja de toda su historia. Su misión actual sigue siendo la de investigar a posibles terroristas, pero después de algunas filtraciones, se ha llegado a la conclusión de que también se espía aleatoriamente a millones de personas inocentes, tanto extranjeras como nacionales; llevándose a cabo una vigilancia masiva innecesaria. Ante estas filtraciones, la NSA se ve en un aprieto y se obliga a llevar a cabo un ejercicio de transparencia, por el que desclasifica cientos de documentos, en los que se determinan algunas operaciones llevadas a cabo por esta institución, y bajo qué base legal. Como bien ya se ha comentado, las operaciones de la NSA vienen determinadas por la FISA, pero no explícitamente, por tanto, debe hacerse un análisis respecto si se ha interpretado esta ley, para poder aplicarla, de forma discrecional o de forma arbitraria.

Estas filtraciones han salido a la luz gracias a Edward Snowden, ex analista de la NSA. Estas filtraciones de información han sido necesarias para concretar las tareas llevadas a cabo por la NSA. Debido a estas filtraciones, Snowden ha tenido que salir de Estados Unidos y buscar asilo en diferentes estados, ya que le acusaban de varios delitos contra el espionaje, que podrían perjudicar la seguridad nacional[65].

La primera intercepción de información se publicó en el periódico The Guardian el 6 de junio de 2013[6667]. Consistía en una orden judicial secreta de la FISC, por la que se obligaba a la compañía Verizon a desviar todas sus llamadas a la NSA, por tal de poderlas controlar.[68] A pesar de ello, quizá la información más relevante que sacó a la luz fue la existencia de los programas PRISM y XKEYSCORE, por los que se vigilaban y espiaban a millones de personas, tanto a nivel nacional como internacional, incluyendo a líderes políticos. Muchas más filtraciones salieron a la

[65] BHAT, Neha. *Passenger 17A: The Snowden, Asylum and the Surveillance-Privacy Debate*, Washington D.C.: Rochester: Social Science Research Network, agosto del 2013.
[66] CLAYTON NEWELL, Bryce; TENNIS, Joseph T. *Me, my Metadata, and the NSA: Privacy and Government Metadata Surveillance Program*, Washington D.C.: Proceedings of the 2014 iConference, Pp. 345-55.
[67] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order Consultado en fecha 05/05/2015.
[68] ANEXO 1: Autorización judicial por la que se obliga a la empresa de telecomunicaciones Verizón a desviar todas sus llamadas a la NSA.

luz, pero lo que consiguió Edward Snowden fue demostrar que la NSA no cumplía con la legalidad, y si lo hacía, lo hacía de una forma discrecional. Por ejemplo, respecto a la orden judicial para la interceptación de llamadas de Verizón, basándose en la Sección 215, de una forma discrecional, casi pasando la línea hacia la arbitrariedad, ya que permite la interceptación de negocios privados de empresas, a favor de la inteligencia nacional.

Así, una vez que salieron a la luz estas informaciones, muchos activistas se pronunciaron totalmente en contra de la NSA, alegando que no respetaba la legalidad, y que por tanto, vulneraba la Cuarta Enmienda de la Constitución. De esta manera, organizaciones sin ánimo de lucro han decidido presentar una querella criminal contra la NSA, por la que se determina que la vigilancia masiva vulnera la Primera y la Cuarta Enmienda.[69] Entre estas organizaciones cabe destacar el grupo Wikimedia, el cual se ve totalmente involucrado, ya que según información revelada por Snowden, los usuarios del grupo Wikimedia podían ser investigados[70], también la organización estadounidense American Civil Liberties Union (ACLU), Amnistía Internacional, PEN American Center, entre otras. Cabe determinar, que anteriormente se habían presentado demandas y querellas contra la NSA por parte de la ACLU, pero no prosperaron.

Recientemente, en concreto el 7 de mayo de 2015, el Segundo Circuito del Tribunal Federal de Apelaciones ha dictado sentencia determinando que el programa de investigaciones telefónicas llevadas a cabo por la NSA es ilegal. Este tribunal ha entendido que no es suficiente la interpretación de la base legal por la que actúa la NSA, y que en consecuencia, al no existir aprobación por parte del Congreso respecto el programa de intervención de llamadas telefónicas, no es legal. Así, determina que este programa es probablemente inconstitucional, y que por tanto vulnera el derecho a la intimidad y a la privacidad de los ciudadanos estadounidenses. A pesar de ello, el tribunal ha decidido que no es conveniente paralizar la continuación del programa, ya que la *USA Partiot Act* tiene vigencia hasta junio, y que si el Congreso es inteligente deberá, o crear una ley que avale la

[69] https://blog.wikimedia.org/2015/03/10/wikimedia-v-nsa/ Consultado en fecha 05/05/2015.
[70] https://www.aclu.org/files/natsec/nsa/20140722/Why%20Are%20We%20Interested%20in%20HTTP.pdf consultado en fecha 05/05/2015.

actuación de la NSA, y en consecuencia todos los programas que lleven a cabo, o que, por otra parte, declare la inconstitucionalidad de los programas de la NSA y no permita usarlos[71].

Por tanto, se puede determinar mediante estas acciones, la preocupación que nace, a nivel nacional, respecto la funcionalidad de la NSA, ya que la sociedad conocía la misión de esta institución, la cual se ocupaba de espiar a extranjeros, por tal de mantener la protección nacional. Pero a partir de las filtraciones de Snowden, los ciudadanos saben que pueden ser investigados, y que se les vulnera su derecho a la intimidad y privacidad, ya que el gobierno ha interpretado la FISA discrecionalmente, casi pasando el límite de la arbitrariedad: interceptando llamadas a nivel nacional, controlando los movimientos por geolocalización dentro del territorio nacional, investigando los perfiles de usuarios en internet de nacionales estadounidenses o creando autorizaciones judiciales que no se encuentran en el marco de las competencias de la FISC.

4. Metodología de vigilancia de la National Security Agency

Tal y como expresa uno de los documentos claves de la NSA[72], el cual se puede encontrar en su página web, la metodología de vigilancia que lleva a cabo dicha institución sigue un patrón, aunque la orden ejecutiva 12333 les permita utilizar infinidad de programas de vigilancia. Esta metodología se divide en seis pasos. El primer paso consiste en la vigilancia extranjera, es decir, se pone en marcha un protocolo que determina que personas o entidades extranjeras pueden tener cierta relación el terrorismo. El siguiente paso, consiste en crear una red de vigilancia que incluya un seguimiento de la persona u organización determinada en el primer paso, y por tanto, encontrar a posibles personas que estén en contacto con él, entendiéndose que pueden ser también terroristas (aquí es donde se podría investigar a un ciudadano estadounidense). El tercer paso consiste en identificar el medio de comunicación por el que se comunican: radio, redes sociales, correo electrónico, teléfono… Directamente relacionado con el punto anterior, también la

[71] http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf Consultado en fecha 07/05/2015.
[72] National Security Agency. *The National Security Agency: Missions, Authorities, Oversight and Partnerships, Op. Cit.*

NSA debe identificar la infraestructura de telecomunicaciones utilizadas para transmitir dichas comunicaciones. Por tanto, la tarea de la NSA será considerar cuales son las vulnerabilidades de los medios de comunicaciones y de la infraestructura de telecomunicaciones, y como último paso, la NSA decidirá qué programa se ajusta más para poder infiltrarse en dichas comunicaciones, o creará uno nuevo si los de su colección no son los óptimos.

Así pues, para conocer la metodología de espionaje de la NSA es imprescindible conocer los programas utilizados para ello, y, realmente, sin las revelaciones de Snowden no se sabría casi nada, ya que, como se ha comentado anteriormente, el ex analista de la NSA ha hecho que esta institución desvelara ciertos documentos para que los ciudadanos intuyeran una transparencia, quizá un poco falsa, pero sí, transparencia, y conocer algunos de los programas. Por tanto, en este trabajo se dará una pequeña referencia de los programas más conocidos, usados y criticados; quizá en estos programas es donde se encuentran las reticencias de todos los estadounidenses y, sobre todo, de los estados extranjeros.

En primer lugar, desde el punto de vista más amplio, se encuentra el programa de almacenamiento masivo de metadatos doméstico y extranjero, que incluye desde llamadas de teléfono, emails, mensajería instantánea, comunicaciones de radio, etc. En base a la sección 215 de la *USA Patriot Act*, todas las llamadas telefónicas pueden ser escuchadas, ya que es considerada una cosa tangible, igual que con cualquier otro medio telemático. Por tanto, esta norma le da a la NSA la capacidad para investigar las actuaciones de cualquier persona, siempre que exista una orden judicial; estas órdenes judiciales son demandadas de forma amplia, es decir, se pide al FISC que haga una autorización, por ejemplo, para investigar todas los emails enviados desde Manhattan. Esto crea lo que se denomina investigación masiva de metadatos, es decir, al investigar a tantos millones de personas, se crea un volumen de información innecesaria, y por tanto, se tienen que crear mecanismos para limitar la información, por tanto se crean los programas específicos de vigilancia, como son el PRISM, el XKEYSCORE o el TEMPORA[73]. A pesar de ello, la NSA, a partir del 11 de septiembre ha creado un mecanismo infalible para conocer todas las

[73] WOLFSON, Stephen Manuel. *The NSA, AT&T, and the Secrets of Room 641A*, Ohio: A journal of law and policy for the information society, Vol. 3:3, 2007/08, Pp. 414-417.

comunicaciones, sobre todo las telefónicas. Este método no es otro que contratar a empresas privadas por tal de interceptarlas: el ejemplo más claro es el de AT&T, y el de la conocida habitación 641A, o Study Group 3 Secure Room. Basándose, en la sección 215 de la *USA Patriot Act*, el gobierno estadounidense firma contratos con empresas privadas por tal de poder llevar a cabo su investigación, y uno de los contratos más importantes es el firmado con AT&T (empresa de telecomunicación telefónica de Estados Unidos), por el que todas las comunicaciones realizadas por sus clientes se copiaban para la NSA. En la séptima planta del 611 de Folsom Street, se encuentra el centro regional de AT&T de San Francisco, por donde pasa todo el tráfico de llamadas nacionales. En 2003, el ex técnico de AT&T Mark Klein[74], descubrió que todo el flujo de información bajaba hasta el sexto piso, en concreto en la habitación 641A, donde recogía una copia de todas las comunicaciones interceptadas, las cuales se redirigían a la NSA[75].

A partir del método general, se crean los programas específicos, como el PRISM. El 6 de junio de 2013 The Washington Post[76] y The Guardian[77] revelaron la existencia de este programa, el cual accede a los datos establecidos en los en las empresas privadas más importantes de internet, como son Google, Facebook o Yahoo. El mismo día, en una rueda de prensa, Adam Clapper, directo de la NSA, reconoció la existencia de este programa, el cual estaba amparado por la sección 215 de la USA Patriot Act, en base a que, tal y como se ha explicado anteriormente, según esta norma el gobierno tiene potestad a acceder a negocios jurídico de empresas privadas, por tal de garantizar la protección nacional[78]. El día 9 de junio de 2013 se hizo pública la figura de Edward Snowden y expresó que la FISC había exigido a la empresa Verizon la copia de todas las llamadas telefónicas nacionales

[74] https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf Consultado en fecha 26/04/2015.
[75] CLOTHIA, Tom. *Five Eyes of Surveillance*, Autralia: Control Publications, Vol. 109, diciembre del 2014, Pp. 16-18.
[76] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ Consultado en fecha 26/04/2015.
[77] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Consultado en fecha 26/04/2015.
[78] BOWDEN, Caspar. European Parlament: Directorate general for internal policies policy department c: citizens' rights and constitutional affairs. *The US National Security Agency (NSA) surveillance programmes. (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental right*.
http://fas.org/irp/eprint/eu-nsa.pdf Consultado en fecha 05/05/2015.

e internacionales[79]. Por tanto, lo que se consigue con este programa es que la NSA pueda recopilar datos de la esfera privada de las personas, gracias a las grandes empresas tecnológicas, entre las que destacan Apple, Microsoft, Facebook o Yahoo, y consecuentemente, sus programas como son Outlook o Gmail. Gracias a Snowden se reveló como se espiaba por el programa de investigación PRISM, el cual fue publicado finalmente por la NSA.[80]

Directamente relacionado con el programa PRISM, debe mencionarse el programa XKEYSCORE. Este es uno de los programas más completos de la NSA, ya que entre sus funciones se encuentra la posibilidad de indexar todo tipo de contenido de internet y extraerlo en sus ordenadores, mediante los cables de fibra óptica enterrados en el fondo de los océanos. Por ejemplo, una de sus funciones principales es la de determinar en qué idioma escribe o habla la persona investigada para determinar si en el contenido se encuentran palabras claves, como terrorismo, yihadista, entre otras.[81] Una de las particularidades más importantes de este método de vigilancia, es que tal y como expresa Graham, no es necesaria la autorización judicial pertinente para la investigación[82]. Igual que el programa PRISM, el funcionamiento de este programa también fue destapado por Edward Snowden[83].

Por último, aunque existen más programas como UPSTREAM, STELLAR WIND o MAINWAY, debe explicarse la base de datos llamada FASCIA, en las que se recogen millones de datos, que determinan la localización, en todo el mundo, de posibles terroristas, a partir de sus teléfonos móviles, gracias al programa CO-TRAVELER. Su funcionamiento es sencillo. A partir del teléfono móvil de una persona, clasificada como objetivo por la NSA, se encuentra su localización en una ciudad concreta, gracias a las torres de comunicación, a las cuales, los teléfonos

[79] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order Consultado en fecha 05/05/2015.
[80] ANEXO 2: Diapositivas del funcionamiento del PRISM.
[81] GONZALEZ LUIS, Alfonso. *Análisis de los programas de vigilancia en internet*. Universitat Oberta de Catalunya, 13 de junio de 2014. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/36601/6/agonzalezluisTFM0614memoria.pdf Consultado en fecha 05/05/2015.
[82] GRAHAM, Stephen. *Surveillance and Intelligence Gathering In the United States: Impact and Implications On Privacy*, Utica: Capstone Project Submitted to the Faculty of Utica College, Diciembre del 2013, Pp. 5.
[83] https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf Consultado en fecha 05/05/2015.

móviles envían señales continuamente (esto es posible a la cooperación de empresas de telecomunicaciones). El siguiente paso es determinar a qué torre envía señales el móvil en concreto, por tal de acotar la localización, y así poder determinar las posibles personas que cooperan con el objetivo, gracias a la misma intercepción de las señales de sus teléfonos móviles[84]. Estos datos de posible cooperación y geolocalización se archivan en la FASCIA: es inimaginable la capacidad de esta base de datos, ya que cada día, a nivel mundial, se recogen, aproximadamente, cinco millones de localizaciones de móvil por día[8586].

5. Relación de España con la National Security Agency

Concretada la posición española durante la Segunda Guerra Mundial, dando apoyo al eje, Estados Unidos apartó sus relaciones internacionales con España. A pesar de ello, en la segunda parte del franquismo, el gobierno franquista consideró necesaria la reintegración al bando occidental, después de años de separación. Así, firmaron ambos estados unos convenios, llamados los Pactos de Madrid o hispano-norteamericano, a partir del año 1953. Estos convenios consistían en unos acuerdos de paz, pero con unas condiciones, que consistían en la cesión de cuatro bases militares a favor de Estados Unidos, a cambio de ayuda económica y militar[87]. A partir de este momento es cuando empiezan las grandes relaciones exteriores, y la consecuente cooperación entre ambos estados. Esta cooperación se da, sobre todo, a través de varios convenios bilaterales, entre los que destacan el acuerdo sobre usos civiles de la Energía Atómica de 1955, el Foreign Leaders Program, el International Education Exchange Program de 1958, Acuerdo entre el Reino de España y los Estados Unidos de América para la mejora del cumplimiento fiscal internacional y la implementación de la Foreign Account Tax Compliance Act o el Convenio sobre

[84] http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/ Consultado en fecha 27/04/2015.
[85] GELLMAN, Barton; SOLTANI, Ashkan. *NSA tracking cell phone locations worldwide, Snowden documents show.* Concord Monitor. 4 de diciembre de 2013. http://www.concordmonitor.com/news/politics/9649281-95/nsa-tracking-cell-phone-locations-worldwide-snowden-documents-show Consultado en fecha 08/05/2015.
[86] http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html Consultado en fecha 27/04/2015.
[87] PIÑEIRO ALVÁREZ, Mª del Rocío. *Los Convenios hispano-norteamericanos de 1953*. Historia Actual Online (HAOL), Núm. 11 (Otoño, 2006), 175-181. 15 de octubre de 2006.

Cooperación para la Defensa en 1988, el cual ha sido posteriormente modificado en dos ocasiones, a través de los Protocolos de Enmienda de 10 de diciembre de 2002 y de 10 de octubre de 2012[88]. Pero quizá el acuerdo más importante ratificado por ambos estados, respecto el tema de investigación y secretismo, es el Acuerdo sobre Seguridad de la Información Militar, Clasificada entre España y los Estados Unidos de América de 1984, por el que se determina la necesidad de cooperación entre ambos estados para la confidencialidad de algunos documentos secretos[89].

Cabe determinar que, en virtud de estos convenios y acuerdos bilaterales, las relaciones entre España y Estados Unidos se han visto reflejadas en varios ámbitos. Uno de los grandes ámbitos ha sido la cooperación en defensa: durante la guerra de Afganistán y la guerra de Irak, España ha sido un aliado claro para los Estados Unidos. A pesar de ello, la cooperación económica y fiscal es excelente[90] y la cooperación en materia de seguridad social es muy beneficiosa[91].

Por tanto, se entiende que la cooperación entre Estados Unidos y España ha sido siempre muy fructífera: en el momento que más se estrechó la relación fue a consecuencia del sufrimiento a raíz de un atentado en cada estado, primero Estados Unidos en 2001, y después España en 2004. Así, la cooperación contra el terrorismo constituyó una de las claves entre estos estados. Por ejemplo, hoy día, la lucha contra el yihadismo es compartida entre ambos estados, y más raíz después de la concreción de Barcelona como capital de células yihadistas "dormidas"[92].

Para combatir contra el terrorismo, igual que Estados Unidos creó la NSA, España constituyó lo que se conoce como el Centro Nacional de Información (CNI). Estas dos instituciones llevan a cabo la misma función: evitar los ataques terroristas, mediante investigación y espionaje. La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, concreta el funcionamiento de ésta y determina en

[88] http://spanish.madrid.usembassy.gov/es/ru/relaciones/tratados-bilaterales.html Consultado en fecha 06/05/2015.
[89] http://www.cni.es/comun/recursos/descargas/EEUU_Texto_BOE.pdf Consultado en fecha 06/05/2015.
[90] Convenio para evitar la doble imposición entre España y Estados Unidos, hecho en Madrid el 22 de febrero de 1990.
[91] Convenio de Seguridad Social entre España y Estados Unidos.
[92] https://wikileaks.org/gifiles/docs/14/1405797_-os-spain-ct-spanish-daily-says-barcelona-becoming-hotbed-of.html Consultado en fecha 06/05/2015.

su artículo 1 "El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones". Como se desprende de este artículo, la actuación del CNI basa su actuación, aunque no se entienda explícitamente, en la protección nacional, tal y como hace la NSA. Para llevar a cabo dichas funciones, e investigar a una persona concreta, el CNI, en virtud de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, se determina la necesidad de autorización judicial. Tal y como establece el artículo 1, el Secretario de Estado Directo del Centro de Inteligencia debe pedir una orden judicial al magistrado del Tribunal Supremo competente para poder investigar a una persona, y por tanto, para tomar medidas contra los derechos fundamentales, recogidos en la Constitución, respecto la intimidad y la privacidad. Tal y como establece el punto 4 del apartado segundo de la disposición adicional única de esta ley, por la que se modifica el artículo 127 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, será competencia del Pleno del Poder Judicial determinar el magistrado, de la Sala de lo Penal Segunda o Sala de lo Contencioso-Administrativo Tercera, los cuales serán los competentes para decidir y emitir sobre dichas autorizaciones.

Respecto el CNI, también cabe aducir que, tal y como establece el apartado c) de su artículo 4 de su Ley reguladora, una de las funciones inherentes a esta institución es la de "Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos". Por tanto, ante la buena cooperación internacional entre Estados Unidos y España, es necesaria una colaboración en el ámbito de la investigación y vigilancia de ciudadanos potencialmente terroristas. Por tanto, tal y como se determina en los documentos aportados por Snowden, España ha cooperado con la NSA, para que esta lleve a cabo sus operaciones. Uno de los documentos aportados por Snowden ha sido una autorización de la FISC de 2010, por la que se aprueba la investigación a estados y organizaciones de estas, entre los

que se encuentra España[93]. En este documento queda claro que no existe colaboración para algunos asuntos, a pesar de ellos, España se encuentra dentro del sofisticado grupo 14-eyes: existen tres grupos respecto la cooperación con la NSA, primero está el grupo 5-eyes, el 9-eyes y el 14-eyes[94]. Otro documento descatalogado[95] certifica que España era considerada por la NSA, como un Estado con el que se establecía una "focused cooperation", es decir, que entre España y Estados Unidos existe una cooperación específica. Directamente relacionado, otro de los documentos filtrados por Snowden, fue el denominado "Spain last 30 days"[96], por el que se desprende en un gráfico la investigación de la NSA en España, la cual lleva a determinar la cooperación entre ambos estados. En este documento se determina la investigación de más de 60 millones de llamadas en España desde el 10 de diciembre de 2010 hasta el 10 de enero de 2011. Pero, ¿realmente esta investigación desproporcionada a ciudadanos españoles es legal?

Primero debe hacerse referencia al Ordenamiento Jurídico estadounidense. Este establece, en la sección 702 de la FISA, la cual establece que es posible investigar a los extranjeros residentes dentro de Estados Unidos, a los no residentes en Estados Unidos y a los estadounidenses residentes fuera de su territorio. Por tanto, la sección 702 de la FISA da carta blanca al poder ejecutivo para poder investigar a cualquier persona u organización, incluso, como se ha dicho anteriormente, a los jefes de estado y políticos de estos terceros estados[9798]. De esta manera cabe establecer que, considerando y aplicando el ordenamiento jurídico norteamericano es legal investigar a ciudadanos españoles.

Respecto el Ordenamiento Jurídico español, debe hacerse una tarea de investigación amplia, ya que no hay documentos doctrinales que determinen la posible

[93] ANEXO 3: Autorización judicial para investigar a terceros estados y organizaciones.
[94] *Eyes wide open: executive sumary*. *Special report.* https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf Consultado en fecha 09/05/2015.
[95] ANEXO 4: Documento que establece que España coopera con la NSA.
[96] ANEXO 5: *Spain last 30 days*.
[97]https://www.eff.org/files/2014/06/30/fisa_amendments_act_summary_document_1.pdf Consultado en fecha 09/05/2015.
[98] Existen varios documentos clasificados de la NSA que determinan que en base a la Sección 702 se pueden investigar a los ciudadanos y organizaciones extranjeras. https://s3.amazonaws.com/s3.documentcloud.org/documents/1211012/faa-fg-cert-2010-a-dni-ag-certification.pdf https://s3.amazonaws.com/s3.documentcloud.org/documents/1211013/faa-fg-cert-2010-a-nsa-dirnsa-affidavit-training.pdf Consultado en fecha 06/05/2015.

cooperación entre el CNI y la NSA, a pesar de ello, existen suficientes indicios para dar fe de ello. Primero debe determinarse, que tal y como publicó el diario el MUNDO, el 30 de octubre de 2013[99], el CNI fue el encargado de facilitar el espionaje masivo a la NSA. Directamente relacionado, una filtración de Wikileaks determinó que el CNI y la NSA estaban en contacto continuamente: en este informe se recopilaba una comunicación entre un agente del CNI y la NSA, por la que se indiciaban las posibles reacciones de los pakistanís, residentes en España, por la muerte de Bin Laden.[100].

Así, desde un punto de vista crítico puede determinarse que España no coopera con Estado Unidos, sino que el CNI trabaja y recopila información de ciudadanos españoles para la NSA, remarcándose así la figura de Estados Unidos reconocida internacionalmente como *Big Brother*. Por tanto, ¿es legal la intervención de la NSA en España, según el Ordenamiento Jurídico español?

El primer texto legal que se debe tener en cuenta es el Convenio entre el Reino de España y los Estados Unidos de América sobre cooperación para la Defensa de 1 de diciembre de 1988, anejos y canjes de notas, texto revisado por Protocolo de Enmienda de 10 de abril de 2002[101]. De este texto se extrae la teoría de *Big Borther* que antes se ha comentado: España cede a Estados Unidos la base de Rota, por tal de que Estados Unidos pueda investigar y llevar a cabo misiones militares, tanto aéreas como navales. A pesar de ello, a España también se le ceden una serie de derechos, consistentes, por ejemplo, tal y como expresa su artículo 18, en que Estados Unidos comparta la información extraída en la base de Rota. Respecto la cooperación entre ambos países, respecto los servicios de inteligencia, cabe hacer mención al artículo 2.3 y al 12 de este convenio. De acuerdo con la primera parte del artículo 2.3, es necesaria una cooperación en materia de enseñanza sobre mecanismos de inteligencia (no se lleva a cabo, ya que el CNI tiene unos programas de vigilancia peores a los de la NSA). La importancia de este artículo se encuentra

[99] http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html Consultado en fecha 06/05/2015.
[100] https://wikileaks.org/gifiles/docs/76/766355_united-states-americas-spanish-intelligence-service-fears.html Consultado en fecha 06/05/2015.
[101] http://www.defensa.gob.es/Galerias/politica/seguridad-defensa/ficheros/DGL-ConvenioCoopDefensaEEUU.pdf Consultado en fecha 06/05/2015.

en su segunda parte donde se determina que "*se fomentarán los intercambios en el campo de la inteligencia militar*". Respecto el artículo 12.2 del convenio se determina que "los cuerpos de inteligencia estadounidenses podrán cooperar físicamente con los cuerpos españoles, siempre que los asuntos que se investiguen sean "de interés mutuo y lleven a cabo investigaciones criminales que afecten a personal o bienes de los Estados Unidos". De estos dos artículos se desprende la necesidad de cooperación entre ambos estados, pero por un motivo concreto: para llevar a cabo investigaciones criminales y militares. Por tanto, según este cuerpo no es legal que la NSA, ni la misma CNI a favor de Estados Unidos, puede llevar a cabo una investigación y una recopilación de metadatos masivas de los ciudadanos españoles. Por otra parte, también debe tenerse en cuenta el Acuerdo sobre Seguridad de la Información Militar, Clasificada entre España y los Estados Unidos de América de 1984, por el que sólo se tiene en cuenta la clasificación de la información militar, tal y como se determina en el título, por tanto, los datos extraídos de las investigaciones actuales, no se pueden regular según este texto legal. Asimismo, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, determina en su artículo 22.2 "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad". Por último, también debe hacerse hincapié en la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia, ya que tal y como establece su artículo 3 "El Gobierno determinará y aprobará anualmente los objetivos del Centro Nacional de Inteligencia mediante la Directiva de Inteligencia, que tendrá carácter secreto", objetivos propuestos anualmente, que serán evaluados por la Comisión del Congreso de los Diputados, en virtud del artículo 11.4[102] del

[102] "La Comisión a que se refiere este artículo conocerá de los objetivos de inteligencia establecidos anualmente por el Gobierno y del informe que, también con carácter anual, elaborará el Director del Centro Nacional de Inteligencia de evaluación de actividades, situación y grado de cumplimiento de los objetivos señalados para el período anterior".

mismo texto legal, y por la Comisión Delegado del Gobierno para Asuntos de Inteligencia, tal y como establece el apartado b) del artículo 6.4 de la Ley Reguladora del CNI[103]. Por tanto, a pesar de que la Directiva de Inteligencia sea de carácter secreto, existen límites para que los objetivos del CNI no exceda la legalidad: existe un doble control general, primero por parte del Gobierno y del Congreso de los Diputados, y un control específico para cada caso concreto, que lo lleva a cabo el poder judicial, tal y como se ha explicado anteriormente. Por tanto, volviendo al tema que nos ocupa, si tanto el Gobierno, como el Congreso de los Diputados y el Tribunal Supremo hubiesen dado el visto bueno a una investigación a ciudadanos españoles, sin motivo alguno, tanto por la NSA como el CNI, se estaría vulnerando el derecho a la intimidad recogido en la Constitución española. Por tanto, es difícil concretar si se ha determinado o no en la Directiva de Inteligencia del CNI la cooperación entre Estados Unidos y España en materia de espionaje masivo, recopilando miles y miles de metadatos sin un índice concreto, pero tanto si se determinara en dicha Directiva[104], como no lo recogiera se vulneraría el derecho a la privacidad personal y familiar, reconocido como derecho constitucional, a todos los investigados sin una causa justa.

En conclusión, debe determinarse que según el Ordenamiento Jurídico español la investigación masiva está prohibida, únicamente podría ser legal dicha investigación si se recogiera como objetivo la cesión de datos a la NSA, en la Directiva de Inteligencia, y siempre que vaya directamente relacionado con un ataques terrorista, una investigación policial o para evitar posibles actos criminales. Por tanto, una recopilación de datos masivos, cedidos a la NSA, debería determinarse como un incumplimiento e interpretación incorrecta de los textos jurídicos expresados, y en consecuencia, la Constitución.

[103] "Corresponde a la Comisión Delegada: Realizar el seguimiento y evaluación del desarrollo de los objetivos del Centro Nacional de Inteligencia".

[104] Es difícil que el Congreso de los Diputados haya dado el visto bueno a una investigación masiva, ya que esta cámara siempre tiene que actuar de buena fe y velar por los derechos de todos los ciudadanos españoles.

6. Conclusiones

El primer debate abierto durante este trabajo es la ponderación entre seguridad y libertades. Como se ha comentado, los Estados tienen la capacidad y el deber de garantizar la seguridad ciudadana, restringiendo algunas libertados, pero ¿dónde se encuentra el punto óptimo entre garantizar las libertades de los ciudadanos mediante un control? Desde un punto de vista subjetivo, considero que la funcionalidad de la NSA, consistente en garantizar la seguridad nacional, y por ende, evitar actos terroristas, no es proporcional a la limitación de derechos que causa. Es decir, una investigación masiva de personas, garantiza extremadamente la seguridad nacional, a pesar de ello, las libertades, como es en este caso el derecho fundamental a la intimidad, se ven fuertemente restringidas. Por tanto, llevándose a cabo un extensivo espionaje de terroristas y no terroristas, el gobierno de Estados Unidos está vulnerando el derecho a la privacidad, tanto a los ciudadanos estadounidenses, como a los extranjeros. Ante esta vulneración de dicho derecho fundamental, se ha creado una consciencia moral que critica las funcionalidades de la NSA. De esta manera, tanto organizaciones como particulares han interpuesto demandas, denuncias y querellas ante los juzgados competentes, debido a la restricción de sus derechos fundamentales. Tal y como se h explicado en la parte final del trabajo, la NSA ha investigado en España, hecho que ha llevado a un particular a interponer querella criminal, dentro del territorio español, contra la misma NSA y el CNI[105].

Quizá, uno de los temas más importantes, el cual ha dado cierta independencia a la NSA, son las autorizaciones que debe emitir la FISC, para que dicha institución pueda llevar a cabo las investigaciones pertinentes. En un primer momento, las autorizaciones eran nominativas, pero a partir de la reforma de la FISA, y después de la Orden Ejecutiva secreta de Bush, que permitía a la NSA espiar sin la autorización correspondiente, se determiní la necesidad de que estas autorizaciones judiciales debían ser de ámbito más general. Es decir, que las autorizaciones no fuesen emitidas para investigar a una persona concreta, sino que se determinarían en dichas autorizaciones colectividades de personas, como por ejemplo, de un listado de Estados terceros a los que se puede investigar, incluyéndose así a

[105] ANEXO 6: Querella criminal contra la NSA y el CNI.

terroristas y a no terroristas, y consecuentemente, investigándose a personas que no tienen nada que ver con las organizaciones terroristas. Esto viene dado por la necesidad principal de la NSA, que no consiste en otra cosa que en llevar a cabo una investigación masiva a nivel mundial para evitar posibles ataques terroristas. Por tanto, con el fin de garantizar los derechos a todos los ciudadanos lo más adecuada sería que el Congreso regulase las funciones de la NSA, para evitar un control arbitrario e indiscriminado de la totalidad de la sociedad mundial. De esta manera, llega a plantearse diferentes cuestiones respecto la licitud y legalidad de las funciones de la NSA, y por tanto, si realmente su única y exclusiva función es la de la lucha contra el terrorismo. A pesar de ello, lo único cierto es que la NSA recopila infinidad de datos de los cuales la mayoría no se analizan, tal y como Snowden señala en una de sus entrevistas: "Buscamos un alfiler en un pajar, pero la verdad es que no entendemos la paja".

Estados Unidos es la primera potencia de control y liderazgo mundial, tanto a nivel económico como político, por tanto se ha convertido en el aliado que todo Estado quiere tener. Así, ha incorporado una gran red de inteligencia para poder investigar y espiar a nivel internacional, por tal de garantizar su propia seguridad nacional, convirtiéndose en lo que se ha determinado como *Big Brother*: investiga a cualquier otro Estado para poder evitar ataques terroristas en el seno de su territorio. Uno de los Estados que ha cooperado para evitar el terrorismo ha sido España, ya que es uno de los aliados de esta gran súper potencia mundial. España ha facilitado el espionaje masivo de sus ciudadanos a Estados Unidos, con la finalidad de que éste pueda controlar y garantizar su propia seguridad nacional.

Una vez establecida, a lo largo del trabajo, la base legal, podría determinarse la licitud o ilicitud de las funciones de investigación de la NSA, pero por la extensión del trabajo este tema no se contemplará, al igual que la constitucionalidad de los programas y las funciones de la NSA, como las actitudes tomadas desde la Unión europea con la finalidad de evitar la restricción de derechos de sus ciudadanos.

Por último, cabe hacer hincapié en si es necesaria la intervención de las fuerzas de inteligencia en la cotidianidad de las vidas de las personas. Desde un punto de vista subjetivo, considero que sí es necesaria per o con ciertos límites, es decir, no es

correcto que el gobierno estadounidense haya dado rienda suelta a la NSA para que lleve a cabo investigaciones masivas de ciudadanos estadounidenses y extranjeros, sin prueba alguna de que exista una relación con organizaciones terrorista. Si se establecieran filtro y límites reales, como por ejemplo, que existiese un objetivo concreto para investigar a una coerta persona, y que la FISC expidiera autorizaciones nominativas, sería una investigación coherente y con las funciones de la NSA: evitar el terrorismo. Por tanto, es necesaria la intervención de las fuerzas de inteligencia, pero restringiendo los derechos y libertades de los ciudadanos lo mínimo posible. Por ejemplo, debe estacarse la figura del CNI, respecto la intercepción de las células yihadistas, que querían llevara a cabo en Cataluña ciertos ataques terroristas. Ciertamente, no se tiene conocimiento de si investigaron a personas que no eran terroristas, o si se llevó a cabo una investigación masiva para llegar hasta esto, pero como no sale tanto información a la luz del CNI, debe determinarse que la actuación de esta institución ha sido brillante, y se ha hecho uso eficiente de sus facultades por tal de reprimir dicho intento de ataque terrorista.

7. Bibliografía

- *Administration White Paper. Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act*. August 9, 2013.
- BECCARIA, Cesare. *De los Delitos y de las Penas*, Salamanca: Alianza Editorial, 2004.
- BHAT, Neha. *Passenger 17A: The Snowden, Asylum and the Surveillance-Privacy Debate*, Washington D.C.: Rochester: Social Science Research Network, agosto del 2013.
- BLACKSTONE, Sir William. *Commentaries on the laws of England (1769)*, Chicago: University of Chicago Press, cop., 1979. Facsim. Of the first ed. of 1765-1769
- BOWDEN, Caspar. European Parlament: Directorate general for internal policies policy department c: citizens' rights and constitutional affairs. *The US National Security Agency (NSA) surveillance programmes. (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU*

citizens' fundamental right. http://fas.org/irp/eprint/eu-nsa.pdf Consultado en fecha 05/05/2015.

- BURR, William. *The United States, China, and the Bomb.* National Security Archive Electronic Briefing Book Nº1. http://nsarchive.gwu.edu/NSAEBB/NSAEBB1/nsaebb1.htm Consultado en fecha 04/04/2015.
- CLAYTON NEWELL, Bryce; TENNIS, Joseph T. *Me, my Metadata, and the NSA: Privacy and Government Metadata Surveillance Program,* Washington D.C.: Proceedings of the 2014 iConference.
- CLOTHIA, Tom. *Five Eyes of Surveillance*, Autralia: Control Publications, Vol. 109, diciembre del 2014. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ Consultado en fecha 26/04/2015.
- *Cryptologic Almanac 50th Aniversary Series. The Creation of NSA - Part 2 of 3: The Brownell Committee.* https://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_Creation_of_NSA_Part_3.pdf Consultado en fecha 30/03/2015.
- CURRAN, Rebeca. *The National Security Agency and Domestic Surveillance*, San Francisco: Harvard Model Congress, 2015.
- DONOHUE, Laura K. *Section 702 and the collection of international telephone and internet content*, Cambridge: Harvard Journal of Law & Public Policy, Winter 2015.
- National Security Agency. The National Security Agency: Missions, Authorities, Oversight and Partnerships, 9 de agosto de 2013.
- https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf
- DOYLE, Charles. *Terrorism: Section by Section Analysis of the USA PATRIOT Act.* "Section 206. Roving Surveillance Authority under the Foreign Intelligence Surveillance Act of 1978". 10 de diciembre del 2001.

https://epic.org/privacy/terrorism/usapatriot/RL31200.pdf Consultado en fecha 23/04/2015

- *Eyes wide Open: executive sumary. Special report.* https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf Consultado en fecha 09/05/2015
- GELLMAN, Barton; SOLTANI, Ashkan. *NSA tracking cell phone locations worldwide, Snowden documents show*. Concord Monitor. 4 de diciembre de 2013. http://www.concordmonitor.com/news/politics/9649281-95/nsa-tracking-cell-phone-locations-worldwide-snowden-documents-show Consultado en fecha 08/05/2015.
- GONZALEZ LUIS, Alfonso. *Análisis de los programas de vigilancia en internet*. Universitat Oberta de Catalunya, 13 de junio de 2014. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/36601/6/agonzalezluisTFM0614memoria.pdf
- GRAHAM, Stephen. *Surveillance and Intelligence Gathering In the United States: Impact and Implications On Privacy*, Utica: Capstone Project Submitted to the Faculty of Utica College, Diciembre del 2013.
- HANYOK, Robert. *Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964*. Cryptologic Quarterly, Edition Winter 2000/Spring 2001, Vol. 19, No. 4 / Vol. 20, No. 1. https://www.nsa.gov/public_info/_files/cryptologic_quarterly/Skunks.pdf Consultado en fecha 31/03/2015.
- HILL, Eleanor; *The FBI's Handing of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2011*. 24 de septiembre de 2002. http://www.intelligence.senate.gov/021017/hillunclass.pdf Consultado en fecha 04/04/2015.
- HOWE, George F. *The Early History of NSA*: National Security Agency, 18/09/2007. https://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf Consultado en fecha 20/03/2015.

- JOHNSON, Thomas R., *American Cryptology during the Cold War*. *1945-1989: Book II: Centralization Wins 1960-1972*: National Security Agency: Center for Cryptological History, 1995, Top Secret Umbra.
- LEE, Newton. *Counterterrorism and Cybersecurity: Total Information Awareness*, New York: Editorial Springer, 2013.
- GAINER, Randy. *The NSA's interception of emails and phone calls in the US is unlawful*, Cleveland: Journal of Internet Law, Vol.9 Nº 8, Feb. 2006, Aspen Publishers, Inc
- *Liberty and Security in Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications.* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf Consultado en fecha 04/04/2015.
- *Memorandum of October 24, 1952 for the Secretary of State and the Secretary of Defense*. https://www.nsa.gov/public_info/_files/truman/truman_memo.pdf Consultado en fecha 30/03/2015.
- *NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes*. 9 de agosto de 2013. https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf Consultado en fecha 15/04/2015.
- Office of the Director of National. *ODNI Statement on the Limits of Surveillance Activities Intelligence*. Washington, DC. 16 de junio de 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/880-odni-statement-on-the-limits-of-surveillance-activities?tmpl=component&format=pdf Consultado en fecha 20/04/2015
- PAREJA, Estel·la. *La carta de derechos humanos emergentes: una respuesta de la sociedad civil a los retos del siglo XXI*, Barcelona: Proyecto de la Carta de Derechos Humanos Emergentes en el Institut de Drets Humans de Catalunya, 2007.

- PIÑEIRO ALVÁREZ, Mª del Rocío. *Los Convenios hispano-norteamericanos de 1953*. Historia Actual Online (HAOL), Núm. 11 (Otoño, 2006), 175-181. 15 de octubre de 2006.
- ROLLINS, John. *NSA Surveillance Leaks: Background and Issues for Congress*: Congressional Research Service, 4 de septiembre de 2013. https://www.fas.org/sgp/crs/intel/R43134.pdf Consultado en fecha 20/04/2015
- RUBEL, Alan. *Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy*, Madison. University of Wisconsin, 2006.
- SHANE, Peter. M. *Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance,* Ohio. Journal of Law and Policy for the Information Society, No. 228, November 25, 2013.
- ROLLINS, John. *NSA Surveillance Leaks: Background and Issues for Congress*: Congressional Research Service, 4 de septiembre de 2013.
- SOLOVE, Daniel J. *A Brief History of Information Privacy Law*, Washington D.C. George Washington University Law School Public Law Research, Research Paper No. 215.
- SOLOVE, Daniel J., ROTENBERG, Marc, SCHWARTZ, Paul M. *Information Privacy Law*, Nueva York., Aspen Publishin Co., 2ª edición, 2006.
- SOLOVE, Daniel J. *Reconstructing Electronic Surveillance Law*, Washington D.C.: The George Washington Law Review. Vol. 72:1701, 30/9/2004.
- SOLOVE, Daniel. *Data Mining and the Security-Liberty Debate*, Whashington D.C.: George Washington University Law School, 2008. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2084&context=faculty_publications
- SOLOVE, Daniel J. *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, Stanford: Stanford Law Review, George Washington University Law School, julio del 2010.
- STAPLES, William G. *Encyclopedia of Privacy: volume 1: A-M*. Greenwood Press, London: Greenwood Press, 2007.

- SUÑÉ, Emilio. *Declaración de derechos del ciberespacio*, Madrid: 6 de octubre de 2008.
- *U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973*).
- WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*, Cambridge: Harvard Law Review, Vol. 4, No. 5, 1980.
- WOLFSON, Stephen Manuel. *The NSA, AT&T, and the Secrets of Room 641A*, Ohio: A journal of law and policy for the information society, Vol. 3:3, 2007/08.
- WONG, Katherine. *The NSA Terrorist Surveillance Program*, Cambridge: Harvard Journal on Legislation, Vol. 43, No. 2, 2006.
- YOO, John. *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, Berkeley: UC Berkeley Public Law Research Paper No. 2369192, 1 de diciembre del 2013.
- http://www.cni.es/ Consultado en fecha 13/05/2015.
- https://www.nsa.gov/ Consultado en fecha 13/05/2015.
- https://edwardsnowden.com/es/ Consultado en fecha 13/05/2015.
- https://nsa.gov1.info/dni/index.html Consultado en fecha 13/05/2015.
- http://go.galegroup.com.are.uab.cat/ Consultado en fecha 13/05/2015.
- http://www.factiva.org/ Consultado en fecha 13/05/2015.
- http://www.Proquest.com/ Consultado en fecha 13/05/2015.
- http://www.jstor.org/ Consultado en fecha 13/05/2015.
- http://www.ssrn.com/ Consultado en fecha 13/05/2015.
- https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf Consultado en fecha 26/04/2015.
- http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order Consultado en fecha 05/05/2015.
- https://blog.wikimedia.org/2015/03/10/wikimedia-v-nsa/ Consultado en fecha 05/05/2015.

- https://www.aclu.org/files/natsec/nsa/20140722/Why%20Are%20We%20Interested%20in%20HTTP.pdf consultado en fecha 05/05/2015.
- http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf Consultado en fecha 07/05/2015.
- http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Consultado en fecha 26/04/2015.
- http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order Consultado en fecha 05/05/2015.
- Consultado en fecha 27/04/2015
- http://www.nytimes.com/2005/12/18/politics/18bush.html?pagewanted=all&_r=0 Consultado en fecha 08/04/2015.
- http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html Consultado en fecha 27/04/2015.
- http://spanish.madrid.usembassy.gov/es/ru/relaciones/tratados-bilaterales.html Consultado en fecha 06/05/2015.
- http://www.cni.es/comun/recursos/descargas/EEUU_Texto_BOE.pdf Consultado en fecha 06/05/2015.
- https://wikileaks.org/gifiles/docs/14/1405797_-os-spain-ct-spanish-daily-says-barcelona-becoming-hotbed-of.html Consultado en fecha 06/05/2015.
- https://s3.amazonaws.com/s3.documentcloud.org/documents/1211012/faa-fg-cert-2010-a-dni-ag-certification.pdf Consultado en fecha 06/05/2015.
- https://s3.amazonaws.com/s3.documentcloud.org/documents/1211013/faa-fg-cert-2010-a-nsa-dirnsa-affidavit-training.pdf Consultado en fecha 06/05/2015.
- http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html Consultado en fecha 06/05/2015.
- https://wikileaks.org/gifiles/docs/76/766355_united-states-americas-spanish-intelligence-service-fears.html Consultado en fecha 06/05/2015

- http://www.defensa.gob.es/Galerias/politica/seguridad-defensa/ficheros/DGL-ConvenioCoopDefensaEEUU.pdf Consultado en fecha 06/05/2015.
- https://www.eff.org/files/2014/06/30/fisa_amendments_act_summary_document_1.pdf Consultado en fecha 09/05/2015
- http://portal.uexternado.edu.co/pdf/7_convencionesDerechoInformatico/documentacion/conferencias/Los_Derechos_Humanos_en_el_Ciberespacio.pdf Consultado en fecha 07/02/2015.
- http://harvardmodelcongress.org/sf/wp-content/uploads/2014/11/House-Intelligence-NSA-Rebecca-Curran.pdf Consultado en fecha 30/03/2015.

ANEXOS

ANEXO 1

Autorización judicial por la que se obliga a la empresa de telecomunicaciones Verizón a desviar todas sus llamadas a la NSA.

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.

ANEXO 2

Diapositivas del funcionamiento del PRISM.

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted]

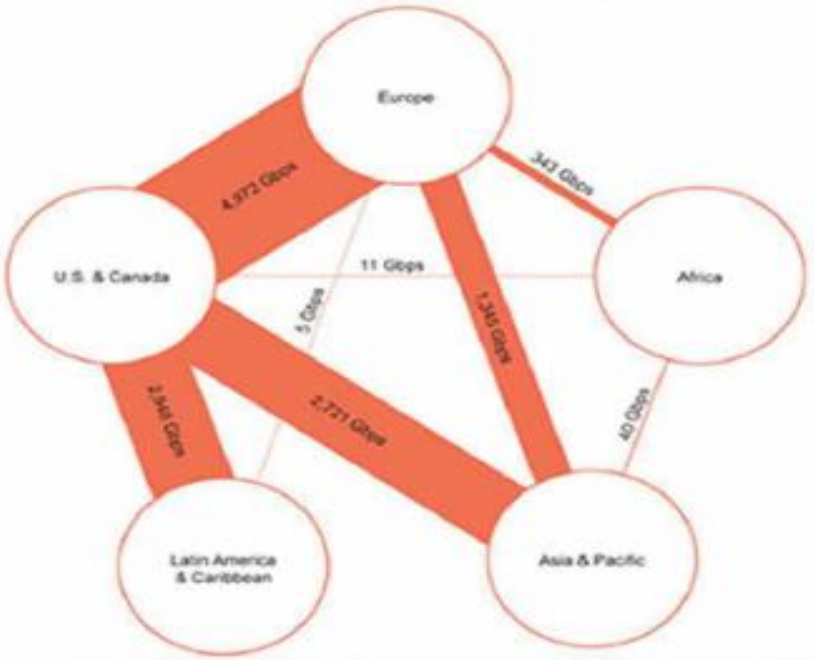
April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction
U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 201
Source: Telegeography Researc

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

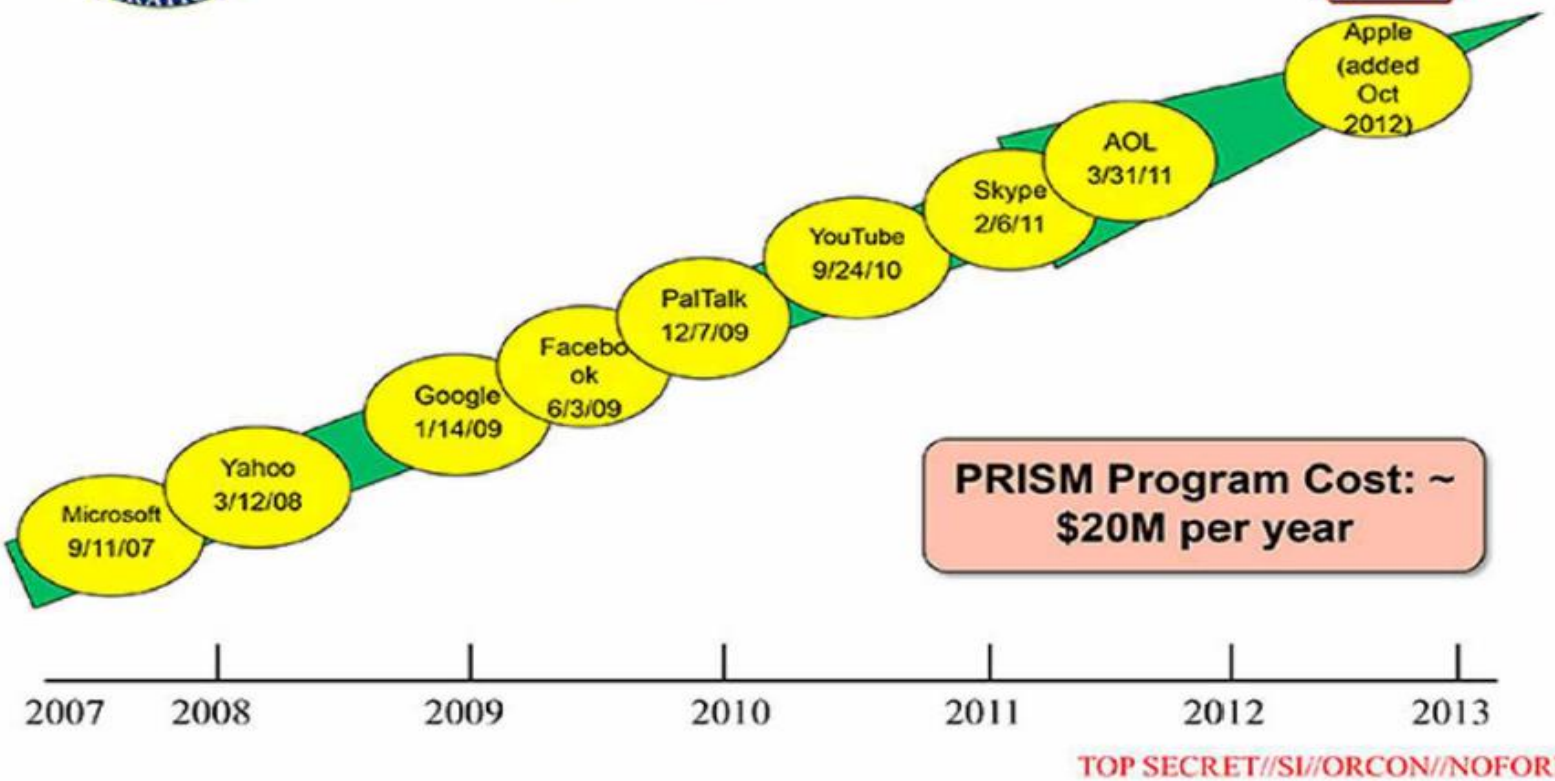
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

ANEXO 3

Autorización judicial para investigar a terceros estados y organizaciones.

U.S. FISC
SURVEILLANCE
2010 JUL 16 AM 11:09
CLERK OF COURT

EXHIBIT F

IN THE MATTER OF FOREIGN GOVERNMENTS, FOREIGN FACTIONS, FOREIGN ENTITIES, AND FOREIGN-BASED POLITICAL ORGANIZATIONS

DNI/AG 702(g) Certification 2010-A

Foreign Governments or Any Components Thereof, Whether or Not Recognized by the United States (50 U.S.C. § 1801(a)(1)):

Afghanistan; Albania; Algeria; Andorra; Angola; Antigua and Barbuda; Argentina; Armenia; Austria; Azerbaijan; Bahamas; Bahrain; Bangladesh; Barbados; Belarus; Belgium; Belize; Benin; Bhutan; Bolivia; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Bulgaria; Burkina Faso; Burma (Myanmar); Burundi; Cambodia; Cameroon; Cape Verde; Central African Republic; Chad; Chile; China; Colombia; Comoros; Congo, Democratic Republic; Congo, Republic; Costa Rica; Cote d'Ivoire; Croatia; Cuba; Cyprus; Czech Republic; Denmark; Djibouti; Dominica; Dominican Republic; East Timor (Timor-Leste); Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Estonia; Ethiopia; Fiji; Finland; France; Gabon; Gambia; Georgia; Germany; Ghana; Greece; Grenada; Guatemala; Guinea; Guinea-Bissau; Guyana; Haiti; Honduras; Hungary; Iceland; India; Indonesia; Iran; Iraq; Ireland; Israel; Italy; Jamaica; Japan; Jordan; Kazakhstan; Kenya; Kiribati; Korea, Democratic Peoples Republic of (DPRK); Korea, Republic of (ROK); Kosovo; Kuwait; Kyrgyzstan; Laos; Latvia; Lebanon; Lesotho; Liberia; Libya; Liechtenstein; Lithuania; Luxembourg; Macedonia; Madagascar; Malawi; Malaysia; Maldives; Mali; Malta; Marshall Islands; Mauritania; Mauritius; Mexico; Micronesia; Moldova; Monaco; Mongolia; Montenegro; Morocco; Mozambique; Namibia; Nauru; Nepal; Netherlands; Nicaragua; Niger; Nigeria; Norway; Oman; Pakistan; Palau; Panama; Papua New Guinea; Paraguay; Peru; Philippines; Poland; Portugal; Qatar; Romania; Russia; Rwanda; Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Samoa; San Marino; Sao Tome and Principe; Saudi Arabia; Senegal; Serbia; Seychelles; Sierra Leone; Singapore; Slovakia; Slovenia; Solomon Islands; Somalia; South Africa; Spain; Sri Lanka; Sudan; Suriname; Swaziland; Sweden; Switzerland; Syria; Taiwan; Tajikistan; Tanzania; Thailand; Togo; Tonga; Trinidad and Tobago; Tunisia; Turkey; Turkmenistan; Tuvalu; Uganda; Ukraine; United Arab Emirates; Uruguay; Uzbekistan; Vanuatu; Vatican City (Holy See); Venezuela; Vietnam; Western Sahara; Yemen; Zambia; Zimbabwe. (TS//NF)

Factions of Foreign Nations, Not Substantially Composed of United States Persons (50 U.S.C. § 1801(a)(2)):

Palestinian Authority; Turkish Republic of Northern Cyprus. (TS//NF)

Classified by: The Attorney General
Reason: 1.4(c)
Declassify on: 15 July 2035

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2010 JUL 16 AM 11:09
LEEANN FLYNN HALL
CLERK OF COURT

EXHIBIT F

IN THE MATTER OF FOREIGN GOVERNMENTS, FOREIGN FACTIONS, FOREIGN ENTITIES, AND FOREIGN-BASED POLITICAL ORGANIZATIONS

DNI/AG 702(g) Certification 2010-A

Foreign Governments or Any Components Thereof, Whether or Not Recognized by the United States (50 U.S.C. § 1801(a)(1)):

Afghanistan; Albania; Algeria; Andorra; Angola; Antigua and Barbuda; Argentina; Armenia; Austria; Azerbaijan; Bahamas; Bahrain; Bangladesh; Barbados; Belarus; Belgium; Belize; Benin; Bhutan; Bolivia; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Bulgaria; Burkina Faso; Burma (Myanmar); Burundi; Cambodia; Cameroon; Cape Verde; Central African Republic; Chad; Chile; China; Colombia; Comoros; Congo, Democratic Republic; Congo, Republic; Costa Rica; Cote d'Ivoire; Croatia; Cuba; Cyprus; Czech Republic; Denmark; Djibouti; Dominica; Dominican Republic; East Timor (Timor-Leste); Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Estonia; Ethiopia; Fiji; Finland; France; Gabon; Gambia; Georgia; Germany; Ghana; Greece; Grenada; Guatemala; Guinea; Guinea-Bissau; Guyana; Haiti; Honduras; Hungary; Iceland; India; Indonesia; Iran; Iraq; Ireland; Israel; Italy; Jamaica; Japan; Jordan; Kazakhstan; Kenya; Kiribati; Korea, Democratic Peoples Republic of (DPRK); Korea, Republic of (ROK); Kosovo; Kuwait; Kyrgyzstan; Laos; Latvia; Lebanon; Lesotho; Liberia; Libya; Liechtenstein; Lithuania; Luxembourg; Macedonia; Madagascar; Malawi; Malaysia; Maldives; Mali; Malta; Marshall Islands; Mauritania; Mauritius; Mexico; Micronesia; Moldova; Monaco; Mongolia; Montenegro; Morocco; Mozambique; Namibia; Nauru; Nepal; Netherlands; Nicaragua; Niger; Nigeria; Norway; Oman; Pakistan; Palau; Panama; Papua New Guinea; Paraguay; Peru; Philippines; Poland; Portugal; Qatar; Romania; Russia; Rwanda; Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Samoa; San Marino; Sao Tome and Principe; Saudi Arabia; Senegal; Serbia; Seychelles; Sierra Leone; Singapore; Slovakia; Slovenia; Solomon Islands; Somalia; South Africa; Spain; Sri Lanka; Sudan; Suriname; Swaziland; Sweden; Switzerland; Syria; Taiwan; Tajikistan; Tanzania; Thailand; Togo; Tonga; Trinidad and Tobago; Tunisia; Turkey; Turkmenistan; Tuvalu; Uganda; Ukraine; United Arab Emirates; Uruguay; Uzbekistan; Vanuatu; Vatican City (Holy See); Venezuela; Vietnam; Western Sahara; Yemen; Zambia; Zimbabwe. (TS//NF)

Factions of Foreign Nations, Not Substantially Composed of United States Persons (50 U.S.C. § 1801(a)(2)):

Palestinian Authority; Turkish Republic of Northern Cyprus. (TS//NF)

Classified by: The Attorney General
Reason: 1.4(c)
Declassify on: 15 July 2035

ANEXO 4

Documento que establece que España coopera con la NSA.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY (Insert #)

Issue Date:
Revised:

(U) SHARING COMPUTER NETWORK OPERATIONS CRYPTOLOGIC INFORMATION WITH FOREIGN PARTNERS

EL MUNDO

(U) PURPOSE AND SCOPE

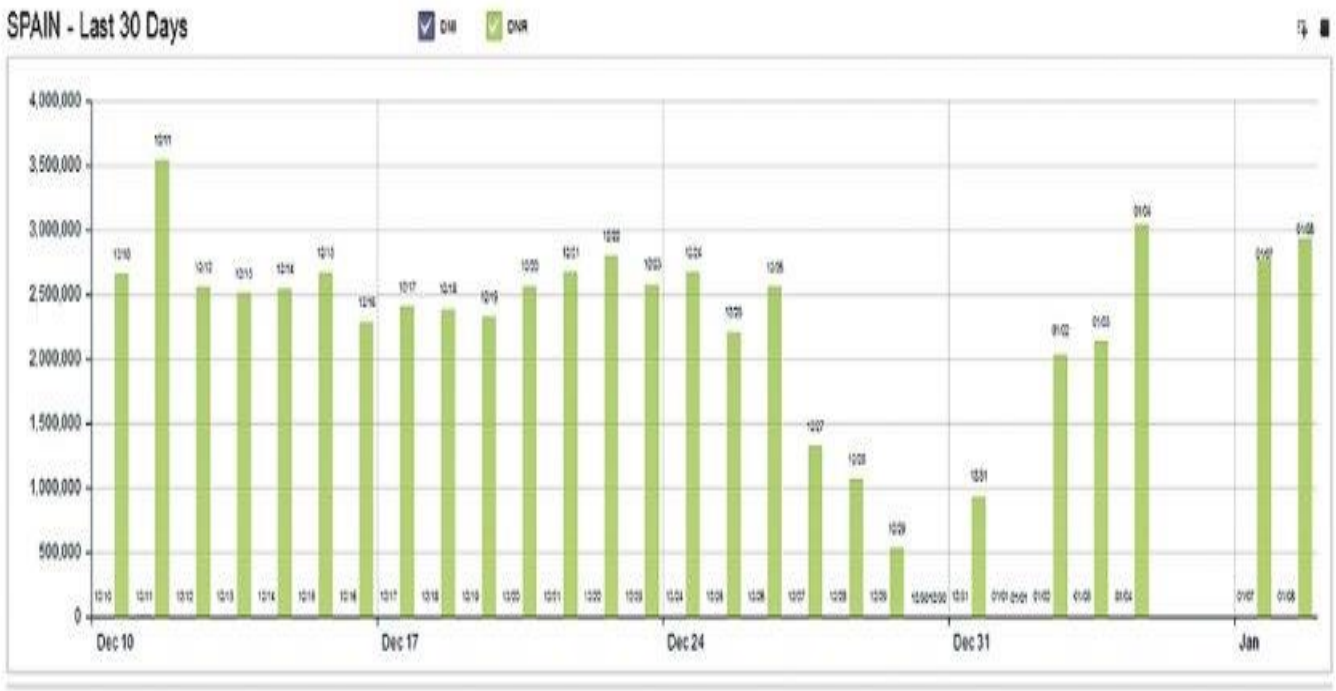
(S//NF) This NSA/CSS policy provides specific guidance for evaluating and initiating Computer Network Operations (CNO) cryptologic cooperation with other countries, generally within existing foreign cryptologic relationships. The policies and procedures outlined in this document are in consonance with the current draft "Director of Central Intelligence (DCI) Guidance on Foreign Cooperation in Computer Network Operations," with DCID 6/7, "Intelligence Disclosure Policy," and with DCID 7/3 "Information Operations and IC-related activities."
(Suggest adding DCI Friends on Friends or take all out as they are references in doc already)

(S//NF) This policy applies to the foreign disclosure of any Computer Network Exploitation (CNE)-related signals intelligence (SIGINT) information and capabilities, as well as Computer Network Defense (CND)-related information and capabilities by any NSA/CSS organization to any foreign entity. This policy also applies to any military-to-military CNE/CND cryptologic

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary
	Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

ANEXO 5

Spain last 30 days.


SPAIN - Last 30 Days
DMI
DNR
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Dec 10
Dec 17
Dec 24
Dec 31
Jan

ANEXO 6

Querella criminal contra la NSA y el CNI

Al Juzgado Central de Instrucción de Guardia en la Audiencia Nacional
Documento en www.cita.es/querella-nsa y www.miguelgallardo.es/querella-nsa.pdf

Miguel Torres Álvarez, (Colegiado 631 del Iltre. Colegio de Procuradores de Madrid) en representación de Miguel Ángel Gallardo Ortiz, la mercantil Cooperación Internacional en Tecnologías Avanzadas (CITA, SLU) constituida en 1996 y la entidad sin ánimo de lucro Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA) constituida en 1992, y bajo la dirección letrada del Dr. José Manuel López Iglesias, según se acreditará mediante "apud-acta" cuando se nos requiera para ello, como mejor proceda en Derecho, **DIGO**:

Que siguiendo instrucciones de mis mandantes, formulo **QUERELLA CRIMINAL** en ejercicio del derecho reconocido en los artículos 270 y siguientes de la Ley de Enjuiciamiento Criminal por los hechos y contra las personas que se mencionan a continuación. En cumplimiento del artículo 783.1 de la citada Ley hago constar que ejerzo cuantas acciones penales y civiles derivan del delito. Dando cumplimiento a lo que determinan los artículos 277 y concordantes de dicha ley, **EXPONGO**:

Primero: Juzgado competente

Se presenta esta querella ante el el Juzgado Central de Instrucción de Guardia de la Audiencia Nacional por lo dispuesto en los artículos 62, 65, y en especial en el punto 1º e (***Delitos cometidos fuera del territorio nacional, cuando conforme a las leyes o a los tratados corresponda su enjuiciamiento a los Tribunales españoles***) de la Ley Orgánica del Poder Judicial.

Segundo: Querellantes

Son querellantes **1.** Miguel Ángel Gallardo Ortiz, ingeniero, criminólogo, licenciado en Filosofía y diplomado en Altos Estudios Internacionales, perito especialista en informática, telemática y criptología forense (según pueden acreditar numerosos juzgados, audiencias provinciales, tribunales y el mismo Consejo General del Poder Judicial CGPJ, que confió al querellante la dirección del curso de formación continuada para magistrados, jueces y fiscales sobre el "*Ámbito Jurídico de las Tecnologías de la Información*" publicándose en el Cuaderno de Derecho Judicial XI de 1996 "*Informatoscopia y tecnologías forenses*" así como "*Métodos de inspección legal de ordenadores e introducción a la informática policial*" en el nº 20 de la Revista Ciencia Policial del Ministerio del Interior). El querellante coautor del libro "*Seguridad en UNIX. Sistemas abiertos e Internet*" **2.** la entidad mercantil Cooperación Internacional en Tecnologías Avanzadas (CITA, SLU) constituida en 1996 y **3.** la entidad sin ánimo de lucro Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA) constituida en 1992, con estatutos en www.cita.es/apedanica

Los tres querellantes tienen como domicilio a efectos de notificaciones en Madrid, C/ Fernando Poo, nº 16, Piso 6º Puerta B, C.P. 28045, **Tel. 902998352** **fax 902998379** y E-mail: miguel@cita.es

Tercero: Querellados

Los querellados son todos aquellos que resulten responsables, por acciones u omisiones que pudieran ser constitutivas de delitos que, directamente o no, puedan haber perjudicado a los querellantes, o a los representados, asociados o no a APEDANICA, o que hayan perpetrado delitos perseguibles de oficio en España o en el extranjero, tanto si son personas físicas, como si los responsables penales fueran personas jurídicas públicas como puedan ser la Agencia de Seguridad Nacional (National Security Agency, NSA) y Agencia Central de Inteligencia (Central Intelligency Agency, CIA) o privadas, como puedan ser Booz Allen Hamilton, Google, Facebook Apple y otras en EEUU, con o sin representante legal en España.

Cuarto: Relación circunstanciada de los hechos

En los últimos días se ha publicado numerosas noticias, pero principalmente en Estados Unidos por The Wasshington Post y en el Reino Unido por The Guardian, sobre el acceso ilimitado de personas contratadas o subcontratadas por la Agencia de Seguridad Nacional (National Security Agency, NSA) y Agencia Central de Inteligencia (Central Intelligency Agency, CIA), como es el caso de la empresa Booz Allen Hamilton, en la que estaba empleado Edward Snowden quien ha revelado que varias empresas, entre las que puede destacarse a Google, Facebook y Apple, han proporcionado acceso a datos, archivos y comunicaciones de no residentes en Estados Unidos, según ha reconocido expresamente el presidente de EEUU, Barack Obama, en declaraciones oficiales amplia y reiteradamente publicadas en varios idiomas.

Lo más relevante penalmente puede ser el denominado programa PRISM o PRISMA de la NSA sobre el que se han publicado controvertidas y alarmantes informaciones. También se ha publicado que:
Google y Facebook piden permiso a EEUU para publicar los datos vinculados con la filtración

Los querellantes APEDANICA, CITA y Miguel Ángel Gallardo Ortiz presentaron una denuncia penal con fecha 16.6.10 ante el Juzgado de Guardia de Madrid por espionaje masivo en numerosas ciudades españolas interceptando comunicaciones en redes inalámbricas WiFi mientras en el "Street View" de Google tomaban imágenes y vídeos en vehículos especiales que hace ya 3 años se descubrió que estaban dotados de antenas que captaban y grababan millones de comunicaciones privadas.

La denuncia repartida al Juzgado de Instrucción 45 de Madrid en Diligencias Previas 2379/10 en auto de 5.8.10 se citó como imputado al representante legal de Google España para que compareciera el 4.10.10, pero desde entonces se ha aplazado varias veces esa comparecencia y además, los abogados de Google, con apoyo de la Fiscalía

han puesto todas las dificultades posibles a las acusaciones personadas, estando esas actuaciones pendientes de resolución en la Sección 7 de la Audiencia Provincial de Madrid Apelación Autos 798/12. Nuestro último escrito para esa causa, de 17.3.13, puede verse en www.cita.es/fernandino y www.miguelgallardo.es/fernandino.pdf

Los querellantes también han denunciado a la Fiscalía y a la Agencia Española de Protección de Datos (AEPD) que el sistema de correo electrónico GMAIL de GOOGLE y la red social FACEBOOK, guardan los datos que sus usuarios han (aparentemente) borrado. En opinión de los querellantes, guardar lo que un usuario decide borrar, y proporcionarlo a terceros, es un presunto delito especialmente doloso porque todos los usuarios de GMAIL y FACEBOOK solamente borran, precisamente, **lo que puede tener más valor como secreto**. Ambas denuncias pueden verse en
www.miguelgallardo.es/gmail.pdf
www.miguelgallardo.es/facebook.pdf

Google y su sistema de correo electrónico GMAIL son especialmente sensibles porque instituciones financieras españolas, como es el singular caso del Banco Bilbao Vizcaya Argentaria (BBVA) dependen tecnológicamente de Google como fácilmente se puede observar buscando la frase "Powered by Google", por ejemplo, en los Webs www.pensionesbbva.com www.bbvaautorenting.com y www.bbvafondos.es entre otros pero también en instituciones publicas españolas en las que muchos españoles estamos obligados a utilizar el correo electrónico de GMAIL, como por ejemplo, la Universidad Complutense de Madrid (UCM) en las direcciones de funcionarios o doctorandos como es el caso del querellante, en el dominio estumail.ucm.es

Google tiene control y responsabilidad sobre varias aplicaciones del Ministerio de Justicia. Los dos últimos Ministros de Justicia, Francisco Caamaño y Alberto Ruiz Gallardón se han relacionado con varios directivos. Pero también es sospechoso que en ninguna de las listas de empresas afectadas por el programa PRISM o PRISMA que se han publicado aparezca IBM, que controla, entre otras muchas aplicaciones, el sistema Lotus Notes utilizado en altas magistraturas y fiscalías según es público y notorio por lo que no solamente es penalmente relevante saber qué sistemas tienen su seguridad comprometidas, sino también cuáles no, y por qué unos sí y otros no.

Por último, ante las recientes noticias publicadas por The Washington Post y The Guardian sobre la NSA y PRISMA, los querellantes se dirigieron al Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) solicitando, sin recibir respuesta, información al respecto mediante correo electrónico enviado a cni@cni.es y también al Centro Criptológico Nacional (CCN-CNI) ccn@cni.es según se ve en www.cita.es/prisma y www.miguelgallardo.es/prisma.pdf

Obviamente, en el momento en el que se redacta esta querella se están produciendo nuevos hechos y más declaraciones relevantes, entre otras, de responsables de servicios de inteligencia europeos, y muy posiblemente en breves fechas deba existir algún posicionamiento, o incluso el ejercicio de otras acciones legales, incluyendo

una posible actuación de oficio por parte del Ministerio Fiscal o procedimientos judiciales asemejables o conexos con esta querella en otros países. Los querellantes tienen intención de actualizar y ampliar esta relación circunstanciada de los hechos relevantes penalmente con el propósito de facilitar su pronta instrucción judicial.

Quinto: Calificación jurídica de los hechos

Sin perjuicio de otras calificaciones jurídicas que puedan concretarse, son relevantes aquí Arts. 197 y ss. del Título X, Capítulo 1º del Código Penal, del **Descubrimiento y revelación de secretos**, considerando especialmente el apartado 3, que dice

El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

También es penalmente relevante el Artículo 31 bis del Código Penal introducido por el apartado cuarto del artículo único de la L.O. 5/2010, de 22 de junio, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 23 junio).

Sexto: Diligencias que se interesan

Los querellantes, como estudiosos de la criptología informática y telemática, tienen el máximo interés en que el juzgador acceda lo antes posible a todos los documentos relevantes sobre el denominado programa PRISMA o PRISM de la National Security Agency (NSA), pero antes de solicitar comisiones rogatorias entendemos que, una vez admitida y ratificada esta querella, son oportunas las siguientes diligencias:

1ª Requerimiento al **Centro Nacional de Inteligencia (CNI)** informe sobre el programa PRISMA de la NSA. Consta que el **Centro Criptológico Nacional (CCN)** del CNI puede facilitar informes a Juzgados Centrales de Instrucción de la Audiencia Nacional (ROJ: SAN 8014/2005). La sede del **Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)** en Internet www.ccn.cni.es está en la Avenida Padre Huidobro s/n, 28071 Madrid, Tel. 913725000.

2ª Que se requiera copia íntegra y testimoniada de todas las actuaciones que se encuentran en la **Sección 7 de la Audiencia Provincial de Madrid Apelación Autos 798/12** procedentes del **Juzgado de Instrucción 45 de Madrid en Diligencias Previas 2379/10** incluyendo el expediente sancionador completo, preferentemente en formato electrónico, iniciado por la Agencia Española de Protección de Datos (AEPD) contra Google España actualmente suspendido por prejudicialidad penal.

3ª **Que se cite en calidad de imputado**, para la mejor defensa y garantía de sus propios derechos, **al representante legal de la mercantil Google España** con domicilio en Plaza Pablo Ruiz Picasso 1, C.P. 28020 Madrid, Tel.: 917486400,

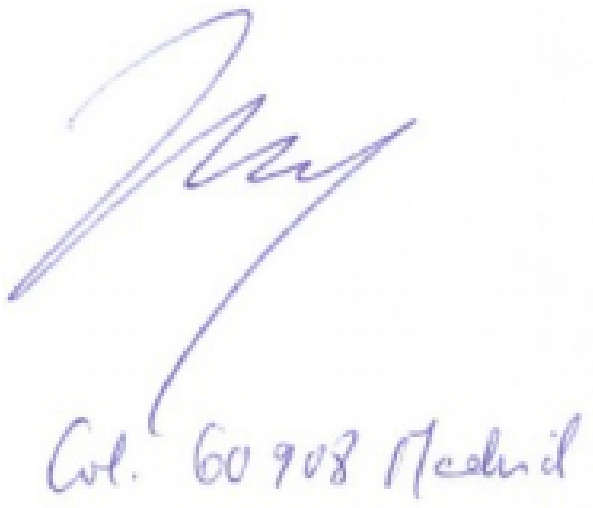
requiriéndole antes toda la documentación de que disponga sobre los presuntos delitos aquí denunciados, y en especial, sobre el programa PRISMA de la NSA considerando que, con o sin permiso del Gobierno de los EEUU, Google España está siempre y en todo caso sometida a la jurisdicción española, a todos los efectos.

Los querellantes se reservan prudentemente proponer otras diligencias una vez que se haya tenido acceso a las actuaciones judiciales, siendo partes personadas.

En mérito de lo anterior, por lo expuesto, suplico al Juzgado que teniendo por interpuesta la presente querella criminal por los hechos y calificaciones, sin perjuicio de que del resultado de las actuaciones se evidenciaran otros hechos delictivos o distintas calificaciones, se digne admitirla y, en su virtud, tener por parte a a todos los efectos legales Miguel Ángel Gallardo Ortiz, la mercantil Cooperación Internacional en Tecnologías Avanzadas (CITA, SLU) constituida en 1996 y la entidad sin ánimo de lucro Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA) constituida en 1992, mediante la representación del procurador de los tribunales que suscribe por designación "apud-acta" cuando se nos requiera para ello, dirigiendo el proceso contra los querellados así como contra cualquier otra persona, física o jurídica, que a lo largo de la causa pudiera aparecer penalmente como responsable, a fin de que en su día y por la autoridad judicial competente se les condene a resultas de esta causa, declarándoles responsables civiles, con costas. Es justo.

OTROSÍ 1 DIGO que conforme a lo dispuesto en el art. 281 de la Ley de Enjuiciamiento Criminal, **esta parte considera que está exenta de prestar fianza**.
OTROSÍ 2 DIGO que los querellantes, el letrado y el procurador **están dispuestos a subsanar cualquier defecto formal de este escrito de querella**, por lo dispuesto en el art. 231 L.E.C., a fin de que prospere pronto y eficazmente.

Por ello, **SUPLICO AL JUZGADO** que tenga por hecha esta manifestación por ser Justicia que reitero en Madrid, a 6 de junio de 2013.



F^do^: Dr. José Manuel López Iglesias, Abogado y Miguel Torres Álvarez, Procurador
Documento publicado en Internet www.cita.es/querella-nsa
y también en www.miguelgallardo.es/querella-nsa