diariolaley Wolters Kluwer

El Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América y la propuesta de *lege ferenda* en el derecho comunitario

Fruela RÍO SANTOS

Abogado y doctorando en Derecho

Diario La Ley, Nº 9004, Sección Tribuna, 20 de Junio de 2017, Editorial **Wolters Kluwer**

Comentarios

Resumen

La situación anterior a FISA. La creación de FISA. The Wall (El Muro). USA Patriot Act. Las reformas FISA. El Tribunal (FISC). Las reglas del procedimiento. Su estudio desde la base legal del Derecho Comunitario.

I. *LA SITUACIÓN ANTERIOR A FISA*

Al poder ejecutivo de los Estados Unidos siempre le ha preocupado vigilar al enemigo, sea nacional o extranjero, sin exigir, con carácter previo, una orden judicial. Entre los ejemplos podemos citar al Presidente de los Estados Unidos, Franklin D. Roosevelt, ordenando a J. Edgar Hoover (el Primer Director del FBI) para que investigase las posibles fuentes de amenazas externas, concretamente de la URSS y Japón (1) . Una vez entrada la Segunda Guerra Mundial, el Presidente de los Estados Unidos, Franklin D. Roosevelt, mandó a Robert Jackson (Fiscal General), para que investigara sin orden judicial, a los extranjeros y no a los nacionales, para que interceptare las llamadas telefónicas con el fin de investigar las amenazas nacionales (2) . Una vez finalizada la Segunda Guerra Mundial, el FBI, en la década de los años 50», ya sea por los derechos adquiridos o así como bajo la premisa del interés nacional, se autorizaba, y no lo hacía por medio de un mandato presidencial sino de forma autónoma, para la interceptación de las llamadas telefónicos, ello implicaba, según algunos autores una vulneración flagrante a la Cuarta Enmienda de la Constitución de los Estados Unidos. Sobre esta cuestión se vino a pronunciar la Corte Suprema de los Estados Unidos, en el asunto *Olmstead vs. United States* (3) , para amparar dicha actuación, al no vulnerar la Cuarta Enmienda, porque las escuchas telefónicas no se realizaban dentro de sus propiedades, ni sobre la persona de manera directa, ni relacionado con los papeles u otros efectos personales de carácter material, sino que se utilizaban cables con el fin de poder obtener información de interés general (4) . La doctrina *Olmstead vs. United States* se mantuvo hasta el año 1967, cuando la Corte Suprema se pronunció en el asunto *Katz vs. United States* (5) , cuando el FBI utilizó una cabina telefónica pública, que utilizaba Katz, para grabar sus conversaciones, y obtener una condena por transmitir informaciones de apuestas. La Corte Suprema revocó la condena de Katz así como dejó sin efecto la anterior doctrina. Lo cierto es que la Sentencia Katz no menciona si pueden existir excepciones, como por ejemplo en los supuestos de seguridad nacional; en ese sentido se pronunció el Juez White, argumentaba que el Presidente de los Estados unidos o el Fiscal General podían autorizar la vigilancia sin orden judicial en interés de la

seguridad nacional. En respuesta a Katz, el Congreso de los Estados Unidos, aprobó la Ley Omnibus de Control de la Delincuencia y Seguridad de las Calles de 1968 [U.S.C. §§ 2510–2520 (1968)] «Crime Control Act», que autorizaba la vigilancia electrónica con una orden bajo estricta supervisión judicial. Pero permitía que el Presidente pudiese *saltarse* dichas garantías en beneficio del interés nacional. La primera vez que la Corte Suprema se pronunció sobre la excepción de seguridad nacional fue en el asunto *United States vs. U.S. District Court (Keith) [United States vs. U.S. Dist. Court, 407 U.S. 297 (1972)],* los acusados, todo ellos ciudadanos estadounidenses, lo fueron por un presunto delito de conspiración que tenía como finalidad destruir propiedades gubernamentales, además, uno de ellos fue acusado de hacer estallar una bomba en una oficina de la CIA en Michigan. La defensa de los acusados requirió al Tribunal para que aportara pruebas de cómo se habían obtenido las grabaciones, es decir, si se habían respetado, o no, las garantías de la *Crime Control Act,* aprobándose la referida prueba, el gobierno tuvo que proporcionar una declaración jurada del Fiscal General John Mitchell, que reconoció que él aprobó las escuchas telefónicas sin orden judicial, pero que las escuchas telefónicas fueron «employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government». Además, el Fiscal General John Mitchell certificó que la divulgación de las conversaciones podía perjudicar la seguridad nacional. El gobierno proporcionó al Tribunal de Distrito, bajo sello, las transcripciones de las conversaciones registradas y registros que indicaba el Fiscal General. El Tribunal de Distrito Falló a favor de los acusados, y el Tribunal de Apelaciones del Sexto Circuito se ratificó en la misma, ordenando un *writ of mandamos (Se debe entender como un mandamiento de un Tribunal Superior dirigido a un Tribunal o Juzgado inferior, o a un organismo o persona, ordenando el cumplimiento de alguna obligación o deber judicial).* De la anterior resolución de la Corte Suprema resalta que la Cuarta Enmienda «no era absoluta en sus términos», por lo que el papel de la Corte era sopesar los intereses relevantes en juego para determinar si las acciones del gobierno eran constitucionales. Así, tres cuestiones merecían especial consideración para la Corte Suprema: 1.- la necesidad de vigilancia del Gobierno para asegurar la seguridad interna nacional; 2.- la posibilidad realizar violaciones en la privacidad y en la supresión de la libertad de expresión; 3.- si el requisito previo de la obtención de una orden judicial impediría la capacidad del Gobierno para proteger al país. La Corte Suprema determinó que un requisito de orden judicial protegería mejor la intimidad y los intereses de la libertad de expresión del individuo. Finalmente, fueron rechazados cada uno de los motivos, y de las alegaciones, por los que el Gobierno ofreció para justificar que la apropiación de la información se basó en una excepción de seguridad nacional, sosteniendo que el Gobierno no había demostrado una razón suficiente para incluir una excepción nacional de seguridad nacional en la Cuarta Enmienda.

II. *LA CREACIÓN DE FISA*

A comienzos de la década de 70, seguía sin existir una normativa que regulase las escuchas telefónicas sin orden judicial, hecho que motivó al Congreso para que crease un marco estatutario diseñado para regular la recopilación de información de inteligencia extranjera. Tenemos que citar a Christopher Pyle, un ex oficial de inteligencia del Ejército, que saltó a la fan a cuando alegó, en medios de comunicación, que los militares americanos se dedicaban a la vigilancia, no reglamentada, de la población civil. Las manifestaciones vertidas originaron una investigación del Senado, pues estábamos ante un hecho social que estaba ganando cada vez una mayor demanda (6) . El segundo hecho versa sobre el escándalo Watergate, del Presidente Nixon, pues se reveló que Nixon utilizó la vigilancia, y sus poderes, sin mandato en nombre de la seguridad nacional para investigar a ciudadanos estadounidenses que eran más una amenaza política para Nixon que una amenaza criminal real (7) . El Comité de la Iglesia reveló más fechorías del Presidente Nixon, pero también informó a la sociedad que el problema era más profundo que el caso Watergate; porque el Presidente Kennedy, por ejemplo, escuchó sin órdenes tanto a Martín Luther King Jr., como a Jimmy Hoffa (8) . En tercer lugar, la compañía telefónica AT&T, amenazó con dejar de cooperar con los funcionarios encargados que llevaban a término las escuchas telefónicas, porque estaban preocupados de que esa cooperación pudiera repercutir negativamente en la empresa (9) . Finalmente, tras la renuncia del Presidente Nixon y la publicación del informe del Comité de la Iglesia, el clima político estaba lo suficientemente maduro para que el Congreso pudiese retomar la voluntad popular. El Senador Edward Kennedy y el Procurador General del Presidente Gerald Ford, Edward Levi, cooperaron para escribir lo que se convertiría en el texto originario FISA (10) . El Senado consideró el proyecto durante los meses previos a las elecciones de 1976, aunque el proyecto final no sería enviado al Presidente Jimmy Carter hasta el año 1978.

III. *THE WALL (EL MURO)*

Con carácter previo decir que El Muro es una metáfora utilizada para describir la incapacidad de los funcionarios federales encargados de hacer cumplir la ley y los funcionarios de inteligencia de coordinar, aconsejar y compartir información entre sí de conformidad con los procedimientos adoptados por el Departamento de Justicia en 1995.

El FISA es un estatuto jurídico complejo. En su nivel más básico, viene a definir los procedimientos necesarios para llevar a cabo la vigilancia electrónica con el fin de obtener inteligencia extranjera. Estos procedimientos no requieren obtener una orden judicial de arresto como sucedería en una investigación criminal bajo el Título III de la Ley de Control de la Delincuencia (11) . Los funcionarios federales en los esfuerzos de contraterrorismo pueden soltar una orden judicial del Título III o una orden de arresto de FISA, las cuales tienen unos requisitos estrictos y contemplan diferentes niveles de secreto.

El Título III de la Ley de Control de la Delincuencia requiere, entre otras cosas, que el funcionario encargado de hacer cumplir la ley someta a un juez una solicitud por escrito que indique lo siguiente: «los hechos y circunstancias» que llevan al funcionario a creer que estamos ante un delito grave, «Ha sido, está siendo o está a punto de ser cometido»; Una descripción de la ubicación «donde se va a interceptar la comunicación»; «Una descripción particular del tipo de comunicaciones que se pretende interceptar»; «La identidad de la persona, si se conoce, que comete el delito y cuyas comunicaciones deben ser interceptadas»; y «una declaración exhausta y completa sobre si otros procedimientos de investigación han sido juzgados o no, o porqué razonablemente parecen no tener éxito si son juzgados o ser demasiado peligrosos». El juez puede exigir más información al funcionario instructor de la causa. Si el juez está convencido de que existe una causa de convicción, de estar ante un posible crimen, y existen motivos suficientes para creer que las comunicaciones sobre el crimen deberían ser interceptadas en el lugar solicitado por el funcionario; y que el resto de medidas, que podrían ser utilizadas, técnicas de investigación fracasaran o bien son demasiado peligrosas, el juez puede autorizar a la agencia a interceptar las comunicaciones objetivo durante un período de hasta treinta días con prórrogas posibles si el funcionario envía una solicitud, argumentando los motivos de la misma. El objetivo debe ser notificado por el funcionario al juzgado en un plazo de noventa días, contados desde la orden judicial concedida.

El FISA debe autorizar la vigilancia electrónica, pero con un rango más reducido de circunstancias admitidas

Al igual que el Título III, el FISA debe autorizar la vigilancia electrónica, pero con un rango más reducido de circunstancias admitidas. La entidad que se vigila debe ser una potencia extranjera o un agente de una potencia extranjera (se utiliza la expresión «poder extranjero»). El objetivo de las comunicaciones debe estar relacionado con «la capacidad de los Estados Unidos de protegerse contra…» así como los esfuerzos de una potencia extranjera para atacar, sabotear, el terrorismo internacional o las actividades clandestinas de inteligencia. Si la información de inteligencia se refiere a un «Persona estadounidense», la información debe ser necesaria para prevenir un ataque, un sabotaje, etc., y no sólo »relacionarse» con la capacidad de los Estados Unidos para hacerlo.

Sin perjuicio de lo expuesto, la normativa regula dos procedimientos que el gobierno puede utilizar para obtener inteligencia extranjera sin una orden judicial.

a) En virtud del primer conjunto de procedimientos, el Fiscal General puede autorizar la vigilancia por un año si el Procurador General certifica por escrito bajo juramento que se cumplen los siguientes requisitos: 1) la vigilancia se dirige únicamente a las comunicaciones entre potencias extranjeras y 2) No existe una probabilidad sustancial de que las comunicaciones de personas estadounidenses sean interceptadas.

b) El segundo procedimiento abarca todas las circunstancias distintas de las contempladas en el primer supuesto, abarcando materias más complejas y amplias. El Fiscal General debe presentar una solicitud ante el Tribunal de Vigilancia de Inteligencia Extranjera (FISC), un tribunal Creado por la FISA y compuesto por jueces de los tribunales federales de distrito nombrados por el Presidente de la Corte Suprema de los Estados Unidos. La solicitud debe contener, entre otros, los siguientes elementos que un juez del FISC puede complementar con requisitos adicionales: 1) la identidad o descripción del objetivo y la duración de la vigilancia necesaria; 2) los hechos que justifican la creencia de que el objetivo es una potencia extranjera o un agente de una potencia extranjera y que las instalaciones a las que se dirige son o serán utilizadas por una potencia extranjera o por un agente de una potencia extranjera; 3) los procedimientos de minimización a utilizar; 4) una descripción del tipo de comunicaciones e información buscadas por la vigilancia;

5) una certificación del Asistente del Presidente para Asuntos de Seguridad Nacional (NSA) afirmando que «el propósito de la vigilancia es obtener información de inteligencia extranjera» y que «tal información no puede obtenerse razonablemente con técnicas de investigación normales».

El juez del FISA debe emitir la orden si determina que existe una causa probable para creer que el objetivo es una potencia extranjera y que las instalaciones a las que se dirige serán utilizadas por esa potencia extranjera. La orden puede autorizar la vigilancia de una potencia extranjera para un año y podrá autorizar la vigilancia de un agente de una potencia extranjera durante un período no superior a noventa días, con prórrogas posibles en ambos casos. El FISA también prevé el establecimiento de una Tribunal de Revisión sobre los actos del Tribunal de Vigilancia de Inteligencia (FISCR), en el caso de que una decisión FISC fuese impugnada. El FISCR no se reunió hasta que tuvo lugar el primer recurso, *In re Sealed Case (In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).),* ocurrió en 2002.

Resumiendo, el FISA concede una autoridad más amplia que la dispuesta dentro del Título III, pero en un rango más estrecho de circunstancias. Se puede presentar una solicitud del Título III a cualquier juez de la Corte de Distrito de los Estados Unidos, mientras que una solicitud del FISA debe ser hecha a un juez FISA especialmente designado. Una orden judicial del Título III debe ser revelada al objetivo dentro de noventa días, mientras que una orden judicial del FISA se mantiene en secreto. Para beneficiarse de este nivel más alto de secreto, el gobierno tiene la carga de demostrar que hay una causa probable para creer que el objetivo es una potencia extranjera y que la información específica se relaciona con la capacidad de los Estados Unidos para protegerse contra el espionaje o terrorismo. Además, el FISA requiere que un alto funcionario del Departamento de Justicia certifique la solicitud, estos requisitos no figuran en el Título III pero se trata de una práctica frecuente.

IV. *USA PATRIOT ACT*

Los atentados terroristas del 11 de septiembre de 2001 generaron la Unidad y el Fortalecimiento de los Estados Unidos mediante la provisión de herramientas apropiadas para interceptar y obstruir la Ley de Terrorismo de 2001 («USA Patriot Act»), que desmanteló considerablemente The Wall.

En primer lugar, la Ley USA Patriot cambió el requisito de la FISA para que un funcionario del gobierno certificara que el objetivo de vigilancia era recopilar información de inteligencia extranjera. Después de la FISA, los tribunales habían interpretado «Propósito» significaba «el propósito primario». Con la adopción de los Procedimientos de 1995, los fiscales y los funcionarios encargados de hacer cumplir la ley fueron prácticamente prohibidos de prestar asistencia o asesoramiento a los funcionarios de inteligencia que se ocupaban de la vigilancia de la FISA. Al cambiar «el propósito« a «un propósito significativo», la USA Patriot Act derribó The Wall (El Muro).

Según la senadora Dianne Feinstein (Case, 310 F.3d 717, 732–33 (FISA Ct. Rev. 2002) quoting 147 CONG. REC. S10591 de 2001.), estos cambios eran necesarios porque «(siendo) más fácil recopilar información de inteligencia extranjera bajo… FISA. En virtud de la legislación vigente, las autoridades sólo pueden proceder a la vigilancia con arreglo a FISA si el objetivo principal de la investigación es recabar información extranjera. Pero en el mundo de hoy las cosas no son tan simples. En muchos casos, la vigilancia tendrá dos objetivos clave: la recopilación de inteligencia extranjera y la recopilación de pruebas para un proceso penal. Determinar qué propósito es el propósito «primario» de la investigación puede ser difícil, y sólo se hará más a medida que coordinamos nuestra inteligencia y los esfuerzos de aplicación de la ley en la guerra contra el terrorismo».

La decisión del FISCR sostuvo que esta disposición de la Ley USA Patriot Act era innecesaria porque —para el FISA— «el propósito», sin perjuicio de la interpretación que le dieron los Procedimientos de 1995, nunca significó que la información de inteligencia extranjera no pudiera ser compartida con los agentes de la ley (En 727 «En resumen, pensamos que la FISA aprobada por el Congreso en 1978 claramente no excluía o limitaba el uso o uso propuesto por el gobierno de información de inteligencia extranjera, que incluía pruebas de ciertos tipos de actividades criminales, en un proceso penal»). En otras palabras, The Wall fue una creación de los Procedimientos de 1995 de Gorelick, no una parte inherente de la legislación original de FISA.

El segundo cambio importante de la Ley USA Patriot Act en la FISA tuvo como objetivo directo los Procedimientos de 1995. La Ley USA Patriot Act establecía que, en lo que respecta tanto a las búsquedas físicas como a la vigilancia electrónica, los oficiales federales que ejecutan una orden de detención FISA «pueden consultar a los agentes de la ley federales para coordinar esfuerzos para investigar o proteger contra: Otros graves actos hostiles de una potencia extranjera o un agente de una potencia extranjera»; (2) «sabotaje o terrorismo internacional por parte de una potencia extranjera o un agente de una potencia extranjera»; o (3) «actividades clandestinas de inteligencia por

un servicio de inteligencia o red de una potencia extranjera o por un agente de una potencia extranjera».

Por otra parte, la Ley USA Patriot Act dice que dicha consulta «no impedirá» la certificación requerida que establece que un propósito significativo de la vigilancia es obtener información de inteligencia extranjera.

Según David Kris, esta sección de la USA Patriot Act establecía que «por definición, la coordinación autorizada, por la USA PATRIOT Act, debe promover un propósito de protección contra las amenazas especificadas en la definición de «información de inteligencia extranjera». La coordinación autorizada no puede «excluir» la finalidad de obtener información de inteligencia extranjera; al contrario, es una prueba afirmativa de ese propósito».

V. *LAS REFORMAS FISA*

La Ley FISA ha sido enmendada de manera significativa por la Ley de Autorización de Inteligencia de 1995, por la Ley de Autorización de Inteligencia de 1999, por la Ley USA PATRIOT, por la Ley de Enmiendas de Reautorización Adicional del PATRIOT de los Estados Unidos de 2006, por la Ley de Enmiendas de la Ley de Vigilancia de Inteligencia Extranjera de 2008, y la Ley de Extensión de la FISA.

Recordemos que el FISA se promulgó inicialmente en 1978 y establece procedimientos para la vigilancia física y electrónica y la recopilación de información de inteligencia extranjera. Inicialmente, la FISA se ocupó únicamente de la vigilancia electrónica, pero se ha modificado de manera significativa para abordar el uso de registros varios, búsquedas físicas y registros comerciales.

VI. *EL TRIBUNAL (FISC)*

El Congreso en 1978 estableció el Tribunal de Vigilancia de Inteligencia Extranjera como un tribunal especial y autorizó al Juez Presidente de los Estados Unidos a designar a siete jueces de tribunales federales de distrito para revisar las solicitudes de órdenes relacionadas con investigaciones de seguridad nacional.

Los jueces sirven por períodos escalonados y no renovables por un plazo máximo de siete años, y hasta 2001 procedían de diferentes circuitos judiciales. Las disposiciones para el tribunal formaban parte de la Ley de Vigilancia de Inteligencia Extranjera (92 Stat. 1783), que exigía al gobierno, antes de iniciar ciertos tipos de operaciones de inteligencia dentro de los Estados Unidos, obtener una orden judicial similar a la requerida en el caso penal Investigaciones. La legislación fue una respuesta a un informe del Comité Selecto del Senado para Estudiar las Operaciones Gubernamentales con respecto a las Actividades de Inteligencia (el «Comité de la Iglesia»), que detallaba las acusaciones de abusos de la autoridad ejecutiva para llevar a cabo la vigilancia electrónica nacional en interés de las autoridades nacionales seguridad. El Congreso también estaba respondiendo a la sugerencia de la Corte Suprema

en un caso de 1972 que bajo la Cuarta Enmienda podría requerirse algún tipo de orden judicial para llevar a cabo investigaciones relacionadas con la seguridad nacional.

Los jueces del Tribunal de Vigilancia de Inteligencia Extranjera viajan a Washington, D.C., para escuchar las solicitudes de autorización sobre una base rotatoria

Los jueces del Tribunal de Vigilancia de Inteligencia Extranjera viajan a Washington, D.C., para escuchar las solicitudes de autorización sobre una base rotatoria. Para asegurar que el tribunal pueda convocarse con poca antelación, al menos uno de los jueces debe ser miembro del Tribunal de Distrito de los Estados Unidos para el Distrito de Columbia.

La ley de 1978 estableció también un Tribunal de Revisión de la Vigilancia de Inteligencia Extranjera, presidido por tres jueces de distrito o de apelación designados por el Presidente de la Corte Suprema de Justicia para examinar las decisiones del Tribunal de Vigilancia de Inteligencia Extranjera. Debido al registro casi perfecto del Departamento de Justicia en la obtención de las órdenes de vigilancia y otros poderes que solicitó al Tribunal de Vigilancia de Inteligencia Extranjera, el tribunal de revisión no tuvo ocasión de reunirse hasta 2002.

La USA Patriot Act de 2001 (115 Stat.) vino a ampliar los períodos de tiempo durante los cuales el Tribunal de Vigilancia de Inteligencia Extranjera puede autorizar la vigilancia y aumentó el número de jueces que sirven a la corte de siete a once. Los once jueces deben ser sacados de por lo menos siete *circuitos* judiciales, y no menos de tres deben residir dentro de las veinte millas del Distrito de Columbia.

Las sesiones del FISC son no públicas para considerar la emisión de órdenes de registro bajo FISA. Los procedimientos ante el FISC son *ex parte*, lo que significa que el gobierno es el único partido presente, así en muy pocas ocasiones su solicitud es denegada por el tribunal.

VII. *LAS REGLAS DEL PROCEDIMIENTO*

Las Reglas de Procedimiento para el Tribunal de Vigilancia de Inteligencia Extranjera fueron promulgadas de conformidad con 50 U.S.C. § 1803 (g). Se aplican en todos los procedimientos del Tribunal de Vigilancia de Inteligencia Extranjera. El actual Reglamento del Tribunal de Vigilancia de Inteligencia Extranjera reemplaza tanto el Reglamento de 17 de febrero de 2006 como el Procedimiento de Revisión de Peticiones de 5 de mayo de 2006 presentado de conformidad con la Sección 501 (f) de la Ley de Vigilancia de Inteligencia Extranjera de 1978 modificado. El actual Reglamento entró en vigor el 1 de noviembre de 2010.

El Reglamento está dividido en siete títulos, siendo los siguientes: Título I de los objetivos y las reglas.

Título II de la información de seguridad nacional.

Título III de la estructura y poderes del Tribunal.

Título IV de los asuntos que puede conocer el Tribunal. Título V de las audiencias, órdenes y resoluciones.

Título VI de los procedimientos suplementarios para los procedimientos 50 U.S.C. § 1881a (h). Título VII de los procedimientos suplementarios para los procedimientos 50 U.S.C. § 1861 (f). Título VIII de los procedimientos *En Banc.*

Título IX de los recursos.

Título X de las disposiciones administrativas.

VIII. *SU ESTUDIO DESDE LA BASE LEGAL DEL DERECHO COMUNITARIO*

A nivel europeo es el caso Snowden el que hace cuestionar la confianza en los flujos de datos personales, derivados de las relaciones entre los EEUU y la Unión Europea. Con fecha de 20 de febrero de 2014 se aprueba el Resumen ejecutivo del Dictamen del Supervisor Europeo de Protección de Datos relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo «Restablecer la confianza en los flujos de datos entre la UE y EE. UU.» y relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. Por el que se propone:

> **a.-** una forma eficaz siguiendo las revelaciones sobre los programas estadounidenses a gran escala de recopilación de información de inteligencia y su impacto en la confianza entre la UE y EE. UU.
>
> **b.-** analizar el marco jurídico estadounidense (3), el modo de recogida y el tratamiento ulterior de los datos (4) y los mecanismos de control y de recurso existentes.
>
> **c.-** con arreglo a la «segunda vía», las instituciones europeas podrán formular preguntas a las autoridades estadounidenses relacionadas con la supuesta vigilancia de las misiones diplomáticas y las instituciones de la UE, mientras que los Estados miembros podrán debatir con las autoridades estadounidenses, de forma bilateral, las cuestiones relacionadas con su seguridad nacional.

Posteriormente, el Parlamento Europeo publica en el año 2015 un estudio comparativo entre la normativa europea y de los EEUU de la protección de datos, en la misma se hace alusión a FISA pero no se cuestiona la viabilidad de introducir un tribunal similar en el seno de la Unión Europea. Con posterioridad, en enero de 2017 se publica por el Parlamento Europeo la From Safe Harbour to Privacy Shield, Advances and shortcomings of the new EU-US data transfer rules, que trae causa en la sentencia Schrems de octubre de 2015 del Tribunal de Justicia de la Unión Europea (TJUE), por la que se declaró nula la decisión de la Comisión Europea sobre un «puerto seguro» para la transferencia de datos UE-EE.UU. La Comisión Europea negoció un nuevo acuerdo, conocido como Privacy Shield, y este nuevo marco para la transferencia de datos UE-EE.UU. Fue adoptado en julio de 2016. Esta publicación

pretende presentar el contexto a la adopción de Privacy Shield así como su contenido y los cambios introducido.

La UE solo ha tratado esta cuestión desde el punto de vista del intercambio de flujos de datos personales con los EEUU

Lo cierto es que la Unión Europea solo ha tratado esta cuestión desde el punto de vista del intercambio de flujos de datos personales con los EEUU, pero la cuestión es más seria y relevante, pues debe garantizarse, para lograr una mayor seguridad, a nivel europeo, la existencia de un tribunal que supervise, controle y autorice las interceptaciones electrónicas que atenten, o puedan atentar, contra la seguridad. El problema se suscita en poder autorizar la filtración de información electrónica con la normativa internacional, pues, los estados europeos son parte del Pacto Internacional de Derechos Civiles y Políticos (PIDCP (LA LEY 129/1966)) de las Naciones Unidas, que protege la privacidad y la correspondencia en virtud del art. 17 (LA LEY 129/1966), mientras que el art. 8 del Convenio Europeo de Derechos Humanos (LA LEY 16/1950) (CEDH) se ha interpretado de manera restringida por la vigilancia gubernamental.

La Directiva sobre protección de datos de la Unión Europea (95/46/CE (LA LEY 5793/1995)), sin olvidarnos del Reglamento Europeo de Protección de Datos Personales, y la Carta de los Derechos Fundamentales aplican protecciones de privacidad más sólidas, aunque no en el ámbito de la seguridad nacional, competencia reservada a los Estados miembros.

De este modo, quizás la competencia no pueda ser asumida por la Unión Europea, sino por cada uno de los estados miembros, quien deberán decidir, respetando la normativa nacional e internacional, relativa a los derechos fundamentales, cuándo, cómo y bajo qué procedimientos se puede crear un tribunal similar al FISA de los Estados Unidos, con el fin de garantizar la seguridad nacional en detrimento de una disminución de los derechos fundamentales, especialmente del relativo a la protección de datos personales.

(1)

NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 74 (Official Gov't ed. 2004); Elizabeth Gillingham Daily, Comment, Beyond «Persons, Houses, Papers, and Effects»: Rewriting the Fourth Amendment for National Security Surveillance, 10 LEWIS & CLARK L. REV. 641, 644 (2006).

(2)

Fletcher N. Baldwin, Jr. & Robert B. Shaw, Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law, 17 U. FLA. J.L. & PUB. POL'Y 429, 435 (2006).

(3)

Olmstead vs. United States, 277 U.S. 438, 464 (1928).

(4)

«The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants».

(5)

Katz vs. United States, 389 U.S. 347 (1967).

(6)

CHRISTOPHER M. FORD, Intelligence Demands in a Democratic State: Congressional Intelligence Oversight, 81 TUL. L. REV. 721, 737–38 (2007).

(7)

MICHAEL P. O'CONNOR & CELIA RUMANN, Going, Going, Gone: Sealing the Fate of the Fourth Amendment, 26. FORDHAM INT'L L.J. 1234, 1255 (2003).

(8)

EVAN TSEN LEE, The Legality of the NSA Wiretapping Program, 12 TEX. J. C.L. & C.R. 1, 39 n. 142 (2006).

(9)

DIANE C. PIETTE & JESSELYN RADACK, Piercing the «Historical Mists»: The People and Events Behind the Passage of FISA and the Creation of the «Wall», 17 STAN. L. & POL'Y REV. 437, 448 (2006).

(10)

Funk, Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma - A History, 11 LEWIS & CLARK L. REV. 1112-13 n.35 (2007)

(11)

DAVID S. KRIS, The Rise and Fall of the FISA Wall, 17 STAN. L. & POL'Y REV. 487, 489–94 (2006). Kevin S. Bankston, Only the DOJ Knows: The Secret Law of Electronic Surveillance, 41 U.S.F. L. Rev. 589, 592 (2007).