Universitat Autònoma de Barcelona

LOS SERVICIOS DE INTELIGENCIA
regulación y límites competenciales de la Unión Europea

Director:
Cristina Blasi Casagran

Autor:
Natalia de La-Chica Prieto
(Doble grado UAB-Paris II Assas)

Viernes, 15 de mayo de 2015

Índice

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos
CEDH	Convenio Europeo de Derechos Humanos
CNCIS	Comisión Nacional de Interceptaciones de Seguridad de Francia *(Commission Nationale pour les Interceptions de Sécurité)*
DGSE	Dirección General de Seguridad Exterior de Francia *(Direction Générale de la Sécurité Extérieure)*
EEAS	Servicio Europeo de Acción Exterior *(European External Action Service)*
ELSJ	Espacio de Libertad, Seguridad y Justicia
EU INTCEN	Centro de Análisis de Inteligencia de la Unión Europea
FRA	Establecimiento de Radio de Defensa Nacional de Suecia *(Försvarets radioanstalt)*
GCHQ	Cuartel General de Comunicaciones de Reino Unido *(Government Communications Headquarters)*
MVR	Reducción Masiva de Volumen *(Massive Volume Reduction)*
NSA	Agencia de Seguridad Nacional de Estados Unidos *(National Security Agency)*
PCSD	Política Común de Seguridad y Defensa
RIPA	Ley Reguladora de los Poderes de Investigación de Reino Unido *(Regulation of Investigatory Powers Act)*
SITCEN	Centro Conjunto de Situación para el Análisis de la Inteligencia *(European Union Joint Situation Center)*
SIUN	Inspección Estatal de Inteligencia y Defensa de Suecia *(Statens inspektion för försvarsunderrättelseverksamheten)*
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea

UE	Unión Europea
UNDOM	Tribunal de Defensa e Inteligencia de Suecia *(Underrättelsedomstolen)*
VPN	Red Privada Virtual *(Virtual Private Network)*

Introducción

11 de septiembre de 2001, en Estados Unidos; 11 de marzo de 2004, en España; 7 de julio de 2005 en Gran Bretaña. Los servicios de inteligencia apenas habían absorbido el impacto de estos acontecimientos cuando se vieron inmersos en una nueva era donde las batallas se ganan con la obtención de información.

Cierto es que la información entendida en sentido amplio – cualquier dato relativo a cualquier noticia que sea conocida – ha estado siempre, desde los orígenes, vinculada con los servicios de inteligencia. En todas las épocas, en mayor o menor medida, el gobernante se ha servido de determinadas estructuras con el fin de obtener información para el ejercicio del poder y defenderse de las amenazas del entorno. Desde el empleo de estructuras no especializadas como los ejércitos nacionales, se fue produciendo una transición hacia los conocidos como servicios secretos cuya existencia era negada sistemáticamente por los gobiernos. Pero es solo a partir de la Segunda Guerra Mundial, debido a la incesante preocupación sobre el enemigo del otro lado del Muro y los elementos subversivos que pudiesen surgir entre sus propias poblaciones, cuando nacieron los servicios de inteligencia tal y como los entendemos en la actualidad.

Hoy en día, los servicios de inteligencia son estructuras que forman parte de la Administración del Estado al servicio del gobernante, cuya misión es la transformación de información en inteligencia a través de lo que se conoce como el *Ciclo de la inteligencia*. A lo largo de este proceso la información es evaluada en términos de fiabilidad, analizada, integrada e interpretada con el fin de obtener como producto final inteligencia, la cual será suministrada al gobernante para que pueda tomar las decisiones que estime oportunas con el menor nivel de azar posible.

Sin embargo, aunque la información haya sido siempre un factor indisociable del funcionamiento de los servicios de inteligencia, desde hace una década la importancia del *Ciclo de la inteligencia* ha ido aumentado considerablemente.

Mientras que en el pasado había una escasez de fuentes de información, en la actualidad existe un exceso debido al gran desarrollo de las nuevas tecnologías.

Como consecuencia, los centros de inteligencia tratan con una inmensa cantidad de datos de carácter personal, prácticamente sin ningún tipo de control, lo que pone en peligro el derecho a la protección de datos.

El derecho europeo a la protección de datos, tal y como está configurado, es ineficaz pues se ve sobrepasado por la actuación de los servicios de inteligencia. Es por ello que uno de los retos a los que se enfrenta la Unión Europea es la adopción de otra perspectiva que implica una regulación conjunta de los servicios de inteligencia, pero ¿en qué medida es posible el establecimiento de una regulación europea de lo secreto?

El presente trabajo se estructurará en 2 ejes. Por una parte, se abordará la insuficiencia de la regulación europea en materia de protección de datos obtenidos por los servicios de inteligencia. Por otra parte, se contemplará la posibilidad de un marco legal que haga de EU INTCEN un centro de inteligencia europeo.

Se hará referencia exclusivamente a los servicios de inteligencia de Estados miembros de la Unión Europea, sin perjuicio de que se pueda hacer mención a textos internacionales como el Convenio de 28 de enero de 1981 del Consejo de Europa o el Convenio Europeo de Derechos Humanos ratificado por 47 Estados (todos los Estados miembros del Consejo de Europa), que incluye Estados que no son miembros de la Unión Europea como Rusia o Armenia, entre otros.

I. Los límites en la regulación del derecho a la protección de datos

El desarrollo de las nuevas tecnologías de la información y comunicación junto con la apertura de las fronteras dentro del Espacio Schengen ha convertido el derecho a la protección de datos en una de las principales preocupaciones dentro de la Unión Europea (en adelante, UE). En esta sección se observará tanto la configuración, a nivel europeo, del derecho a la protección de datos, como la actuación de los servicios de inteligencia de los Estados miembros en la era de la información.

1.1. El marco legal europeo en materia de protección de datos

1.1.1. Un marco normativo en evolución

El derecho a la protección de datos es el derecho que toda persona tiene a que permanezcan desconocidos determinados datos relativos a su vida, así como controlar el conocimiento que de ellos tienen los terceros. Su fundamento último es el derecho a la intimidad, el cual tiene una correlación directa con la dignidad humana y la libertad del individuo.

En un primer momento, surgió como una manifestación del derecho a la intimidad, pero la vertiginosa evolución de las nuevas tecnologías de la información y comunicación han desembocado en la necesidad de dotar de una mayor protección al individuo, de tal modo que el derecho a la protección de datos ha ido adquiriendo una mayor importancia hasta convertirse en un derecho autónomo, completamente independiente del originario.

La primera norma sobre protección de datos en la UE se sitúa en Alemania con la *Datenschutz* de 7 de octubre de 1970[1], seguida por la *Datalag* sueca de 11 de mayo de 1973[2]. Estas leyes se centran sobre el espacio físico en que se ubica la información (ordenador y base de datos) y en la necesidad de obtener una autorización previa para su acceso y uso.

Posteriormente, encontramos una segunda categoría de normas – encabezadas por la *Privacy Act* de 1974 de los Estados Unidos[3] – que aportan los principios básicos que deben regir todo tratamiento de datos, como son la necesidad de que el tratamiento esté justificado, el consentimiento del titular, el derecho de acceso y control, así como la obligación de mantener la calidad de los datos y en todo caso, informar en el momento de la recogida de la finalidad de los mismos.
Dentro de esta segunda categoría, se podrían incluir igualmente las normas inspiradas en la Ley francesa de 6 de enero de 1978[4] que aumentan el grado de protección cuando el tratamiento de datos abarca determinados datos personales conocidos como *"datos sensibles"* como son los relativos a la raza, religión, sexo, ideología, etc.

Finalmente, aparece una tercera fase en la evolución del derecho a la protección de datos que, de hecho, constituye el marco normativo europeo actual. Dicha evolución obedece a determinadas circunstancias, como es la aparición el 1 de enero de 1983 de Internet con todo lo que lleva implícito. Otro elemento determinante fue la sentencia del Tribunal Federal alemán de 15 de septiembre de 1983[5], en virtud de la cual se declararon inconstitucionales algunos preceptos de

1 *Datenschutz* (Política de privacidad), 7 de octubre 1970, en la República Federal de Alemania.
2 *Datalag 1973:289* (Ley de datos 1973:298), 11 de mayo 1973, en Suecia.
3 *Public law 93-579-DEC Privacy Act of 1974* (Derecho público 93-579-diciembre Ley de Privacidad de 1974), 31 de diciembre 1974, en los Estados Unidos.
4 *Loi nº 78-17 relative à l'informatique, aux fichiers et aux libertés* (Ley nº78-17 relativa a los datos, archivos y libertades), 6 de enero 1978, en Francia.
5 Sentencia del *Bundesverfassungsgericht* (Tribunal Constitucional) de la República Federal de Alemania 15 de septiembre 1983 *"la proliferación de centros de datos ha permitido gracias a los avances tecnológicos, producir una imagen total y pormenorizada de la persona respectiva – un perfil de la personalidad –, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en un hombre de cristal (...)"*.

la Ley del Censo *"Grundgesetz"* de 1982, que requerían la contestación obligatoria de unos cuestionarios cuyos resultados podían ser utilizados por cualquier administración. A esto se añade la particular necesidad en el ámbito europeo de unificar las disparidades legislativas entre Estados miembros. Todas estas circunstancias permiten entender el contexto en el que surgió el marco normativo europeo del derecho a la protección de datos.

1.1.2. Un marco normativo incompleto

a) La legislación del Consejo de Europa

En razón de la enorme capacidad de los programas de vigilancia en masa para recabar datos personales, han surgido serias preocupaciones sobre la compatibilidad de dichas actividades con el *"Derecho al respeto a la vida privada y familiar"* y en concreto al respeto de la *"correspondencia"* recogido en el artículo 8 del Convenio Europeo de Derechos Humanos[6] (en adelante, CEDH). Aunque este precepto legal no tiene por objeto específico la protección de datos, sí que abarca uno de sus aspectos que es el derecho al respeto de la correspondencia; derecho que ha sido perfilado y desarrollado por el Tribunal Europeo de Derechos Humanos (en adelante, TEDH).

Cuando la demanda supera los rigurosos requisitos de admisibilidad que establecen los artículos 34 y 35 del TEDH, para que sea estimada se ha de considerar que existe una violación de alguno de los derechos contenidos en el CEDH, de entre los cuales se encuentra el derecho a la vida privada y familiar. No obstante, el artículo 8.2 prevé una excepción al derecho a la vida privada y familiar en la medida en que *"esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad*

6 *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales,* CEST nº005, más conocido como la Convención Europea de Derechos Humanos, adoptado por el Consejo de Europa, 4 de noviembre 1950, en Roma.

nacional (...)". En consecuencia el derecho a la vida privada no es absoluto, pero esto no significa que haya una suspensión automática de este derecho en las esferas de la seguridad nacional.

De acuerdo con la consolidada jurisprudencia del TEDH[7], cualquier vigilancia que afecte al derecho a la vida privada debe estar *"en concordancia con la ley",* lo que equivale a que la legislación considerada defina con precisión las categorías de delitos o personas que son susceptibles de estar sometidos a los sistemas de vigilancia, así como los límites en la duración de la misma.

Además, es necesario que la injerencia en la vida privada sirva a un *"objetivo legítimo en una sociedad democrática"* siendo *"necesarias"* y *"proporcionadas"*[8] en relación con el objetivo perseguido.

A estas exigencias "negativas" que implican un deber de no injerencia en la vida privada, hay que añadir también obligaciones "positivas". Los Estados deben establecer las garantías oportunas para prever cualquier posible abuso de poder[9].

De entre las decisiones más relevantes del TEDH, se encuentra la Sentencia del caso Malone[10], por la cual se declara que el procesamiento de los metadatos *"es un elemento integral en las comunicaciones hechas por teléfono. En consecuencia, comunicar dicha información a la policía sin consentimiento de su subscriptor también conduce (...) a una interferencia con el derecho garantizado por el artículo 8"*.

Tradicionalmente los gobiernos tienden a otorgar menos importancia a los metadatos – todo dato relacionado con la comunicación que ha tenido lugar, excepto su contenido – que al contenido de la información, a pesar de que es precisamente en virtud de los metadatos, que determinados sofisticados programas

7 Sentencias TEDH 18 de mayo 2010, caso *Kennedy* c. *Reino Unido;* 1 de julio 2008, caso *Liberty y otros* c. *Reino Unido;* 29 de junio 2006, caso *Weber y Saravia* c. *Alemania, §95.*

8 Sentencia TEDH 26 de marzo 1987, caso *Leaner* c. *Suecia, §58.*

9 Sentencia TEDH 24 de abril 1990, caso *Kruslin* c. *Francia, " Por encima de todo, el sistema (sistema legal francés) no ha dado por el momento las garantías adecuadas contra diversos abusos de poder posibles (...) La ley francesa, expresa o implícitamente, no indica con claridad razonable el alcance y la forma de ejercicio de las facultades pertinentes a atribuir a los poderes públicos (...)" §§35-36.*

10 Sentencia TEDH 2 de agosto 1984, caso *Malone* c. *Reino Unido, §84.*

informáticos identifican patrones de comportamiento. Con esta decisión se otorga, por primera vez, un mismo grado de protección tanto al contenido de la información como a todo lo relacionado con ella como es el número de teléfono o la dirección IP de la persona que está llamando o enviando un email, hora y localización de la información, el asunto, el destinatario, etc.

Pocas son las ocasiones en las que el TEDH se ha pronunciado sobre las actuaciones de los servicios de inteligencia, pero lo cierto es que a éstos también les son aplicables los principios enunciados por el Tribunal. En el asunto *Asociación 21 diciembre 1989 y otros* c. *Rumanía,*[11] el presidente de una asociación que reivindicaba la investigación sobre las víctimas de muerte y daños causados en diciembre 1989, se estima objeto de medidas secretas de vigilancia (escuchas telefónicas) llevadas a cabo por el Servicio de Inteligencia de Rumanía. El Tribunal concluyó que, si bien tal injerencia en la vida privada puede estar justificada por una legislación nacional, dicha legislación ha de cumplir con determinados requisitos; requisitos que en el caso concreto no se cumplían, debido a la ausencia de límite en cuanto al tiempo en que se podían almacenar los datos y a la falta de objetivos específicos que justificaban dichas medidas de vigilancia.
En cambio, en el asunto *Klass y otros* c. *Alemania*[12] el TEDH sostuvo que la legislación controvertida que permitía la vigilancia secreta de correo electrónico, correo postal y telecomunicaciones no violaba el artículo 8 de la CEDH, a pesar de que no se le informó a la persona afectada de las medidas de vigilancia y por consecuencia, esta persona no pudo recurrir a los tribunales una vez que dichas medidas habían finalizado. El TEDH consideró que la legislación que permitía tal vigilancia contenía suficientes garantías contra los posibles abusos y que era necesaria en una sociedad democrática para los intereses de la seguridad nacional.

11 Sentencia TEDH 21 de diciembre 1989, caso *Asociación "21 diciembre 1989" y otros* c. *Rumanía, "(...) la Corte constata que la ausencia de garantías en la legislación nacional propias a garantizar que las informaciones obtenidas por una vigilancia secreta son destruidas a partir del momento en que no se necesitan más para conseguir el objetivo buscado (...) no refleja un objetivo de búsqueda específico, aparte de la vigilancia de exploración general" §174.*

12 Sentencia TEDH 6 de septiembre 1978, caso *Klass y otros* c. *Alemania.*

El Consejo de Europa ha adoptado textos más específicos relacionados con el tratamiento de datos personales como el Convenio nº108[13] que fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Este texto legal establece una serie de principios básicos con el fin de reforzar *"la protección jurídica de los individuos con relación al tratamiento automatizado de datos de carácter personal que les conciernen"*. A los principios recogidos en el artículo 5 del Convenio (tratamiento leal y legítimo, finalidades determinadas y legítimas, proporcionalidad, exactitud, etc.), hay que añadir el contenido del artículo 6 que prohibe el tratamiento automatizado de datos especialmente sensibles como son los que revelan el origen racial, las opiniones políticas, las condiciones religiosas, etc.

El artículo 9 establece una serie de excepciones a los precitados artículos de entre las que se encuentra *"la protección de la seguridad del Estado"*. Este artículo se ha modificado en la propuesta de modernización de la Convención nº108 de 18 de diciembre de 2012[14], el cual se refiere a *"una ley accesible y previsible y constituya una medida necesaria en una sociedad democrática para (...) la protección de la seguridad nacional (...)"*. Aunque no se trata de una modificación sustancial pues *"seguridad del Estado"* y *"seguridad nacional"* son expresiones similares, la redacción de esta disposición se aproxima en gran medida al requisito que impone el TEDH sobre la *"calidad de la ley"*. En efecto, el Tribunal impone que la ley que prevea la restricción al derecho a la protección de datos cumpla con requisitos de *"accesibilidad"* y *"previsibilidad"*[15].

Para finalizar, no se puede dejar pasar por alto el Convenio sobre la Ciberdelincuencia[16] adoptado por el Consejo de Europa en 2001, tras cuatro años de deliberaciones. Ha sido vital para la armonización legislativa en este ámbito,

13 *Convenio para la Protección de los Individuos respecto al Procesamiento Automatizado de los Datos Personales*, CEST nº108, adoptado por el Consejo de Europa, 28 de enero 1981, en Estrasburgo.

14 Propuesta de modernización del Comité Consultivo de la Convención *para la Protección de los Individuos Respecto al Procesamiento Automatizado de los Datos Personales*, adoptada por la vigésimo novena sesión plenaria del Consejo de Europa, 18 de diciembre 2012.

15 Sentencia TEDH 29 de junio 2006, caso *Weber and Saravia* c. *Alemania*.

16 *Convenio sobre la Ciberdelincuencia,* CEST nº185, adoptado por el Consejo de Europa, 23 de noviembre 2001, en Budapest.

pues los Estados parte[17] han tenido que modificar su legislación de forma que consideren delictivas una serie de conductas que se dividen en cuatro grupos (delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos referidos a la falsificación y fraude informáticos; pornografía infantil e infracción de la propiedad intelectual). Es el convenio internacional más influyente en relación con los incumplimientos de la legislación sobre Internet u otras redes de información. También establece los poderes procedimentales que comprenden el registro de redes informáticas y la interceptación de comunicaciones. Pero a diferencia del Convenio nº108, no existen excepciones a su aplicación por razones de seguridad nacional. El Convenio sobre la Ciberdelincuencia obliga, sin excepción alguna, a las partes contratantes a prever en su legislación nacional una protección adecuada de los Derechos Humanos y de las libertades y, en particular, de los derechos garantizados con arreglo al CEDH, como el derecho a la protección de datos.

b) La legislación de la Unión Europea

La UE nació con una pretensión económica, pero ha evolucionado hacia la integración y el reconocimiento de los derechos y libertades. Uno de los puntos más significativos de la integración europea es la elaboración de la Carta de los Derechos Fundamentales de la Unión Europea[18] (en adelante, la Carta) que fue solemnemente proclamada en el año 2000. No obstante, su proclamación no le confirió un carácter jurídicamente vinculante. La adopción del proyecto de Constitución para Europa, firmado en 2004, le habría dado dicho carácter vinculante, pero, como consecuencia del fracaso del proceso de ratificación, siguió siendo una simple declaración de derechos hasta la adopción del Tratado de Lisboa. La Carta pasó a ser jurídicamente vinculante a través del Tratado de

17 El Convenio sobre la Ciberdelincuencia está abierto para la adhesión por parte de Estados no miembros del Consejo de Europa y, a día de febrero de 2015, está en vigor en 6 Estados no miembros del Consejo de Europa: Australia, República Dominicana, Japón, República de Mauricio, Panamá y Estados Unidos.

18 *Carta de los Derechos Fundamentales de la Unión Europea,* C326, 18 de diciembre 2000, proclamada solemnemente por el Parlamento Europeo, la Comisión Europea y el Consejo de la Unión Europea, el 7 de diciembre 2000, en Niza.

Lisboa[19], que establece en su artículo 6.1 que *"tendrá el mismo valor jurídico que los Tratados"*.

La Carta enumera los derechos básicos que la UE ha de respetar, así como los Estados miembros cuando aplican el Derechos de la Unión. De entre las libertades básicas encontramos en el artículo 7 el *"Respeto de la vida privada y familiar"*. Pero, en concordancia con las explicaciones relativas al texto de la Carta[20], el derecho a la vida privada y familiar del artículo 7 de la Carta tiene el mismo sentido y alcance que el artículo 8 del CEDH. Como consecuencia de ello, la vida privada y familiar puede ser objeto de injerencia por la autoridad pública *"en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás"*.

Además de los artículos 7 y 8 de la Carta, una pieza clave en el proceso de armonización europea en materia de protección de datos la constituye la Directiva 95/46/CE[21] relativa a la protección de personas físicas en lo referido al tratamiento – tanto automatizado como manual – de datos personales y a su libre circulación. Su aplicación territorial se amplía más allá de los Estados miembros, incluyendo también a los Estados no miembros de la UE que forman parte del Espacio Económico Europeo, en concreto, Islandia, Liechtenstein y Noruega[22].

La libre circulación de bienes y servicios, capitales y personas en el mercado interior implicaba la libre circulación de datos, la cual no podía llevarse a cabo sin

19 *Tratado de Lisboa* firmado por los representantes de los Estados miembros de la Unión Europea, 13 de diciembre de 2007, en Lisboa que reformó el *Tratado de la Unión Europea* de Maastritch y el *Tratado constitutivo de la Comunidad Europea* de Roma, cuya denominación actual es *Tratado de Funcionamiento de la Unión Europea.*

20 Oficina de publicaciones oficiales de las comunicaciones europeas "*Explicaciones relativas al texto completo de la Carta de los Derechos Fundamentales de la Unión Europea",* del Consejo de la Unión Europea, diciembre 2000, en Luxemburgo.

21 Directiva 95/46/CE, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* del Parlamento Europeo y del Consejo de la Unión Europea, 24 de octubre 1995.

22 Decisión 94/1/CE, *relativa a la celebración del Acuerdo sobre el Espacio Económico Europeo,* del Consejo de la Unión Europea y de la Comisión Europea, 13 de diciembre 1993.

un nivel elevado y uniforme de protección de datos. Es por esta razón que la armonización de las legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. Por consiguiente, los Estados miembros únicamente tienen un limitado margen de maniobra a la hora de aplicar la Directiva.

Además de su función de armonización, la Directiva de protección de datos introduce un órgano de supervisión independiente como instrumento de mejora del cumplimiento de las normas de protección de datos.

De la Directiva se excluye el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas y también cuando el tratamiento tenga por objeto la *"seguridad del Estado, defensa y seguridad pública"*. A pesar de que el artículo 2 de la Directiva proporciona definiciones de términos clave con el fin de facilitar su comprensión y aplicación uniforme, no aparece definición alguna sobre lo que se ha de entender por *"seguridad del Estado, defensa y seguridad pública"*.

Aún con la unificación de la Directiva 95/46/CE, se hacía necesaria la existencia de una norma que regulara de forma más específica el sometimiento de las instituciones y organismos de la UE a la protección de datos porque la Directiva 95/46/CE solo estaba dirigida a los Estados miembros. Esta pretensión dio lugar al Reglamento nº45/2001[23] relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Tras recoger las pertinentes definiciones de conceptos, se establecen una serie de principios básicos relativos a la forma en que los datos son tratados (al igual que en la Directiva 95/46/CE) y también sobre la calidad de los mismos. A este fin, el Reglamento crea una autoridad de control independiente responsable de la vigilancia de los tratamientos de datos personales efectuados por las instituciones y los organismos comunitarios : el Supervisor Europeo de Protección de Datos,

23 Reglamento nº 45/2001/CE, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos,* del Parlamento Europeo y del Consejo de la Unión Europea, 18 de diciembre 2000.

cuyas decisiones son recurribles ante el Tribunal de Justicia de la Unión Europea (en adelante, TJUE).

No obstante, como ocurre con la Directiva 95/46/CE, se establecen una serie de excepciones de entre las que aparece en el artículo 20.1, letra d *"la seguridad nacional, el orden público y la defensa de los Estados miembros"*.

En cuanto a lo relativo a las actuaciones de los servicios de comunicación en las redes electrónicas públicas encontramos la Directiva 58/2002/CE, de 12 de julio de 2002, modificada por la Directiva 2009/136/CE[24]. Su objetivo principal es eliminar el envío de correos electrónicos no solicitados, lo que se conoce como *"spam"* impidiendo que se camufle la identidad del remitente del correo o la utilización de una dirección de expedición falsa. De igual forma, se regulan las condiciones relativas a los programas espías – spyware – que no podrán recoger información sobre los usuarios de Internet, ni tampoco utilizarla, sin consentimiento de los mismos. Por último, regula la imposibilidad de explotar comercialmente los datos relativos a la localización generados por teléfonos móviles, si no es con consentimiento explícito del usuario. Pero, una vez más, se excepciona todo esto cuando prima la seguridad nacional (artículo 1.3).

Finalmente, en el marco de la cooperación policial y judicial en materia penal, es de especial relevancia la Decisión marco 2008/977/JAI[25] del Consejo de la UE, que tiene por objeto blindar protección a las personas físicas cuando sus datos personales sean tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecutar sanciones penales. Su aplicabilidad queda limitada a garantizar la protección de datos en la cooperación transfronteriza entre las autoridades policiales competentes en los Estados miembros. Los datos deberán ser utilizados solamente por la autoridad competente

24 Directiva 2002/58/CE, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas,* 12 de julio 2002, modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de la Unión Europea, 25 de noviembre 2009.

25 Decisión marco 2008/977/JAI, *relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal,* del Consejo de la Unión Europea, 27 de noviembre 2008.

y únicamente para el fin para el que fueron transmitidos o puestos a disposición. El Estado miembro receptor deberá respetar las limitaciones en el intercambio de datos establecidas por la legislación del Estado miembro transmisor. El registro y la documentación de las transmisiones constituyen un deber específico de las autoridades competentes para ayudar a aclarar las responsabilidades derivadas de las reclamaciones. Las transferencias ulteriores de datos recibidos en el transcurso de una actividad de cooperación transfronteriza a terceros, requiere el consentimiento del Estado miembro en el que los datos tienen su origen, aunque existen excepciones en casos urgentes. Sin embargo, la Decisión marco de protección de datos no se aplica en el ámbito de la seguridad nacional.

Desde el año 2012, la Comisión Europea ha propuesto una reforma, que está compuesta por un Reglamento general[26] para la modernización de los principios consagrados en la Directiva 95/46/CE y una Directiva[27] específica sobre el tratamiento de los datos personales en el marco de la cooperación policial y judicial en materia penal. Aunque esta reforma incorpora nuevos mecanismos para reforzar la protección de datos personales dentro y fuera de la UE, tanto en la propuesta de Reglamento como de Directiva se excluye de sus respectivos ámbitos de aplicación el tratamiento de datos personales *"en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, en particular en lo que respecta a la seguridad nacional"*.

En definitiva, puede parecer que los programas de vigilancia llevados a cabo por los servicios de inteligencia de los Estados miembros no están sometidos a la ley europea de acuerdo con la excepción de seguridad nacional y que, por consecuencia, solo les es aplicable la ley nacional. Sin embargo, esta afirmación no es del todo cierta.

---

26 Propuesta de Reglamento *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* del Parlamento Europeo y del Consejo de la Unión Europea, 25 de enero 2012.

27 Propuesta de Directiva *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos,* del Parlamento Europeo y del Consejo de la Unión Europea, 25 de enero 2012.

De acuerdo con el TJUE las limitaciones a los derechos fundamentales – como es el derecho a la protección de datos – tienen que ser interpretadas restrictivamente. El mero hecho de alegar la existencia de motivos de seguridad nacional no es suficiente para justificar la inaplicación de la ley europea de protección de datos en el ámbito de los servicios de inteligencia, sino que hay que demostrar la existencia efectiva de dicha excepción. En el caso *Digital Rights Ireland Ltd y Seitlinger y otros*[28], el TJUE declaró inválida la Directiva sobre la conservación de datos[29], puesto que la retención de datos *"sin ninguna diferenciación, limitación o excepción"* constituye *"una seria injerencia con los derechos fundamentales en el orden legal de la UE, sin que esa injerencia haya sido precisamente circunscrita por disposiciones para asegurar que es efectivamente limitada a lo estrictamente necesario"* (§§57-65). Al imponer la conservación de datos que permiten saber con qué persona y de qué modo se ha comunicado un abonado, determinar el momento de la comunicación, etc. y al permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales, al respeto de la vida privada y a la protección de datos de carácter personal. Además, la Gran Sala consideró que el hecho de que la conservación y la utilización posterior de los datos se efectúen sin que el abonado o usuario registrado sea informado de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante.

De este modo el TJUE no solo ponía fin a la controversia generada por la Directiva de retención de datos, sino que también marcaba un giro en la jurisprudencia en la medida en que aplica de manera rigurosa los parámetros de protección de los derechos y aplica los estándares europeos sobre el derecho a la vida privada y a la protección de datos personales.

28 Sentencia TJUE 8 abril 2014 (asuntos acumulados C-293/12 y C-594/12), caso *Digital Rights Ireland Ltd y Seitlinger y otros.*

29 Directiva 2006/24/CE, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, del Parlamento Europeo y del Consejo de la Unión Europea, 15 de marzo 2006.

c) El concepto de seguridad nacional

El concepto "seguridad nacional" aparece sistemáticamente no solo en los mencionados textos legales sino también en la prensa, en informes sobre política exterior o incluso en discursos políticos pero, ¿qué se entiende por "seguridad nacional"?

A pesar de ser un concepto troncal en el ámbito de la política exterior, no existe un consenso a nivel europeo y mucho menos a nivel internacional de lo que constituye y abarca "la seguridad nacional". La ambigüedad que gira en torno a esta noción obedece a un gran número de factores, como la complicada delimitación del término de "seguridad" que en sí mismo es extremadamente amplio. Simultáneamente, la idea de "amenaza" que es precisamente la que genera la necesidad de seguridad, es profundamente subjetiva y por consecuencia, difícil de definir.

Tradicionalmente, se ha identificado al Estado como el objeto referente de la "seguridad" y se han conceptualizado las amenazas en términos militares emanando de fuera de las fronteras. Siguiendo esta lógica, la vía hacia la seguridad nacional se alcanzaba a través de políticas encaminadas a la adquisición de capacidades militares. Sin embargo, este razonamiento, preeminente durante la Guerra Fría, se ha quedado anticuado pues la globalización y los desarrollos tecnológicos han traído consigo la aparición de nuevas formas de amenaza no militares, como son el ciberterrorismo, el cambio climático, problemas medioambientales, etc.

Retomando la cuestión inicial, considero que el objetivo último de la seguridad nacional es la salvaguarda de la integridad de la nación, en otras palabras se trata de asegurar la protección de todos los elementos que forman parte de un Estado. En concreto, se pueden identificar, tal y como lo puso de relieve el prestigioso

autor Barry Buzan[30], cuatro elementos básicos : su base física (la población y el territorio), la idea de "el Estado" (nacionalidad y organización de ideologías), sus instituciones (toda estructura del gobierno) y finalmente, su soberanía. Al fin y al cabo la "seguridad nacional" no es más que la preservación de un modo de vida entendido en sentido amplio[31]. Por tanto, la excepción de seguridad nacional tiene un objeto a la vez extremadamente amplio y abstracto (la preservación de un modo de vida), es por ello que dar una definición de esta excepción y de lo que abarca sería un gran paso en la regulación de los centros de inteligencia.

En principio la definición debería provenir del legislador nacional, pues la "seguridad nacional" es una materia exclusiva de los Estados miembros. Por tanto, el legislador europeo no tiene competencia para regular este ámbito. No obstante, esto no quiere decir que a nivel europeo no se pueda también proporcionar una definición de lo que se entiende por "seguridad nacional" con el fin de delimitar de una forma más clara y precisa el ámbito de aplicación de la normativa europea. La legislación europea ha de ser respetada por los Estados miembros y, en consecuencia, si determinadas actuaciones llevadas a cabo por sus servicios de inteligencia no entran dentro de lo que calificamos como "seguridad nacional" entonces deberían cumplir con la normativa europea. Por consiguiente, la definición debería ser aportada por las instancias nacionales, pero sobretodo por el legislador europeo pues esto permitiría una mínima armonización.

A mi modo de ver, los vacíos legales que radican en la ausencia de definición sobre lo que se ha de entender por "seguridad nacional" responden a razones puramente políticas, pues es sabido que los gobiernos están completamente opuestos a una mínima injerencia por parte de la UE en materias que son tradicionalmente propias y exclusivas de la administración central del Estado, como es la seguridad nacional. Como consecuencia de ello, los Estados miembros tienen un verdadero margen de discrecionalidad en el sector de la seguridad

30 BUZAN Barry *"People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era",* pp.65-96.

31 HAYCOCK Ronald *"The Evolution of Canadian National Security Policy",* p.1.

nacional; sector que ha sido objeto de críticas por parte de los ciudadanos, sobretodo a partir del verano de 2013 cuando los medios de comunicación desvelaron, a partir de los documentos aportados por Edward Snowden, como los servicios de inteligencia habían realizado actividades de vigilancia electrónicas masivas sobre los ciudadanos de Europa y demás partes del mundo.

1.2. La actuación de los servicios de inteligencia de los Estados miembros

1.2.1. Una vigilancia masiva sistemática

La vigilancia masiva no es un fenómeno nuevo en los regímenes liberales, sobretodo desde la aparición de las nuevas tecnologías y plataformas de extracción de datos que permiten tener acceso a cantidades inimaginables de información. Sin embargo, si hay algo que diferencia a los regímenes democráticos de los autoritarios, son precisamente los motivos y el alcance de la vigilancia. En principio, los servicios de inteligencia de los regímenes democráticos solo llevan a cabo la vigilancia por determinados motivos y sobre individuos específicos. Es por ello que las revelaciones de Edward Snowden son de suma importancia, pues desvelan como los centros de inteligencia han ido demasiado lejos, así como la reticencia de las autoridades políticas a reconocerlo.

Este apartado se centrará en los sistemas de vigilancia de determinados Estados miembros: Reino Unido, Suecia y Francia. Se tratan de Estados miembros que abordan el problema de la articulación de los servicios de inteligencia con las libertades individuales, pero desde perspectivas diferentes. Mientras que Reino Unido encarna el sistema de derecho anglosajón (o *Common Law*), basado en gran parte en el análisis de las sentencias judiciales, Francia sigue el sistema romano francés, también conocido por derecho continental basado sobretodo en la normativa emanada por los poderes legislativo y ejecutivo. En cuanto a Suecia,

representa el modelo escandinavo del bienestar. Aunque el concepto de "Estado de bienestar" tiene más connotaciones políticas que jurídicas, esta idea también ha tenido repercusiones en Derecho, pues el sistema sueco se basa en un equilibrio entre el colectivismo generalizado y un alto grado de libertad individual. De hecho, la figura del Defensor del pueblo surgió en Suecia en 1809 (*"Ombudsman")* para velar por el respeto de los derechos y las libertades fundamentales de las personas frente a los abusos de la Administración Pública. Así, a través de estos tres Estados miembros, que encarnan los principales modelos jurídicos que existen en la UE, podemos obtener una visión global sobre como está regulada la actuación de los servicios de inteligencia.

a) Los servicios de inteligencia y su regulación en Reino Unido

Dentro de la UE, todo indica que el Estado miembro más involucrado en las actividades de vigilancia a gran escala es Reino Unido[32], quizás en gran parte gracias a su estrecha relación con los Estados Unidos. De hecho, es el único Estado miembro de la UE que forma parte – es uno de los *"five eyes"* junto con los Estados Unidos, Canadá, Australia y Nueva Zelanda– del sistema de vigilancia ECHELON. Todo ello hace que Reino Unido se beneficie de una plaza privilegiada en la esfera internacional.

En este Estado la vigilancia es llevada a cabo, principalmente por la agencia conocida como el Cuartel General de Comunicaciones del Gobierno (en adelante, GCHQ), cuyo mandato es trabajar al servicio de *"la seguridad nacional, con especial referencia a la defensa y la política exterior del gobierno de Su Majestad; en los intereses del bienestar económico de Reino Unido; y en apoyo de la prevención y detección de delitos graves"*[33].

32 DIDIER Bigo, CARRERA Sergio, HERNANZ Nicholas, JEANDESBOZ Julien, PARKIN Joanna, RAGAZZI Francesco y SCHERRER Amandine *"UK surveillance: justice, freedom and security in the EU"*.

33 *Intelligence Services Act* (Ley de los Servicios de Inteligencia), 26 de mayo 1994, en Reino

El GCHQ tenía acceso a las comunicaciones obtenidas a través del programa de vigilancia estadounidense PRISM[34], a pesar de que el sistema legal británico prohibe tener acceso a material personal que ha sido obtenido a partir de una compañía establecida fuera de Reino Unido. El programa PRISM tiene como objetivos aquellos ciudadanos que vivan fuera de los Estados Unidos, aunque también se incluyen a los ciudadanos estadounidenses que hayan mantenido contacto con personas que habitan fuera de las fronteras del país. Así, la Agencia de Seguridad Nacional de los Estados Unidos (en adelante, NSA), y en consecuencia el GCHQ, tenían acceso a correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, notificaciones de inicio de sesión, transferencia de archivos, detalles sobre perfiles en redes sociales, historiales de búsqueda, etc.

También se ha revelado que el GCHQ estaba involucrado con la NSA en el programa MUSCULAR[35]. A través de este programa se puede interceptar el tráfico de datos que fluye por medio de los servidores de *Yahoo*, *Google*, *Miscrosoft Hotmail* y *Windows Life Messenger*, de entre otros. El punto de acceso (DS-200B) está situado fuera de territorio estadounidense lo que hace que el programa esté fuera de la jurisdicción de el Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos (también conocido como FISC o FISA Court). Respecto a este programa se dice que numerosos analistas que trabajan en él se quejan de que produce demasiada información, la mayoría de de ella de poco valor.

Igualmente el GCHQ estaba implicado, junto con la NSA, en el programa TEMPORA que otorga acceso a cables de fibra óptica que conduce grandes cantidades de comunicaciones privadas de usuarios de Internet. Se calcula que se instalaron interceptores en alrededor 200 cables de fibra óptica submarinos que llegan a la costa sur oeste de Reino Unido. La información interceptada y procesada eran tanto "contenidos" (se almacenan durante 3 días) de mensajes de emails, historiales de los accesos de internet de los usuarios, etc. como

Unido.

34 BOWCOTT Owen *"UK-US surveillance regime was unlawful for seven years"*.

35 GELLMAN Barton y SOLTANI Ashkan *"NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say"*.

"metadatos" (son guardados durante 30 días) es decir la hora y la fecha de la creación de la información, su creador, el lugar donde fue originada, etc[36].

Desde un punto de vista estratégico el GCHQ controlaba gran parte de las comunicaciones transmitidas a través de Internet. Sin embargo, los proveedores de Internet, conocedores de estas técnicas empezaron a cifrar su tráfico de comunicaciones. A raíz de esta tendencia se creó EDGEHILL; programa de descifrado del tráfico de comunicaciones a través de Internet. En otras palabras este sistema trata de "burlar" la seguridad que ofrecen las redes privadas virtuales (en adelante, VPN). El GCHQ tiene como objetivo descubrir a finales de este año los códigos utilizados por 15 grandes compañías de Internet y 300 VPNs. Asimismo, los analistas de este proyecto están trabajando en el descifrado de las redes de las principales proveedoras de correos web.

Todo este volumen de información recopilado es filtrado a través de la técnica llamada Reducción Masiva del Volumen (en adelante, MVR). Se calcula que aproximadamente el 30% de los datos son eliminados al principio del proceso por ser de poco valor – descargas de música, películas, etc. –. Con los datos restantes se aplican "selectores" que pueden consistir en palabras clave, direcciones de email, números de teléfono, etc. Existen alrededor de 40.000 selectores identificados por el GCHQ.

Los documentos filtrados por Edward Snowden también hacen referencia a otros menos conocidos como el *"Global Telecoms Exploitation"*, el cual da al GCHQ acceso a 600 millones de "eventos telefónicos" al día.

La vigilancia de comunicaciones en Reino Unido está regulada por la *"Regulation of Investigatory Powers Act"* (en adelante, RIPA)[37], la cual establece dos regímenes separados en función del tipo de información. Por una parte, encontramos el contenido de la comunicación cuya interceptación requiere una orden firmada por el Secretario de Estado (válida de 3 a 6 meses) donde se

36 MACASKILL Ewen, BORGER Julian, HOPKINS Nick, DAVIES Nick y BALL James *"GCHQ taps fibre-optic cables for secret access to world's communications"*.

37 *Regulation of Investigatory Powers Act* (Ley Reguladora de los Poderes de Investigación), 20 de julio 2000, en Reino Unido.

especifique o bien un individuo o bien los indicios o las razones que motivan dicha interceptación. No obstante, dicha orden no sería necesaria si estamos ante comunicaciones externas a Reino Unido. En tal caso bastaría con un certificado proveniente del Secretario de Estado que describiese la naturaleza o clasificación del material examinado. Es precisamente esta orden la que rige, en principio, los intercambios de datos con los Estados Unidos – a través del programa PRISM y TEMPORA –. Por otra parte, la RIPA prevé un régimen autónomo para el acceso a "las comunicaciones de datos". Las comunicaciones de datos hacen referencia a las identidades de los individuos, el material, la localización, etc. en definitiva se trata de los metadatos. Respecto a este tipo de información determinadas agencias tienen capacidad de auto autorizar el acceso, de tal forma que no se necesita la precitada orden del Secretario de Estado.

Aunque la RIPA es una legislación que incluye test de proporcionalidad y necesidad antes de que el contenido de la comunicación y los metadatos son interceptados, expertos destacan que *"los estándares de acuerdo con los que estos tests de proporcionalidad son llevados a cabo permanecen principalmente secretos, y aplicados por asesores legales del gobierno y el Secretario de Estado con un limitado poder de control"*[38].

Estas declaraciones no concuerdan con las conclusiones de la investigación realizada por el Comité de Inteligencia y Seguridad del Parlamento. El Comité es responsable del control de las políticas, gasto, administración y operaciones del Servicio de Seguridad (MI5), del Servicio Secreto de Inteligencia (MI6) y del GCHQ. El 17 de julio de 2013, el Presidente del Comité de Inteligencia y Seguridad declaró que las alegaciones sobre la posible utilización por el GCHQ del programa PRISM para obtener acceso a comunicaciones privadas sin la correspondiente autorización eran *"infundadas"*. El Presidente del Comité sostuvo que en cada caso examinado el GCHQ obtuvo la orden correspondiente de acuerdo con la RIPA (órdenes que no han sido publicadas).

38 Declaración del Doctor Ian Brown (Universidad de Oxford), testigo experto en el caso *Big Brother Watch and Others* c. *Reino Unido,* Aplicación nº 58170/13 en la Corte Europea de Derechos Humanos, 27 de septiembre 2013.

No obstante, hay cierta ambigüedad en sus declaraciones pues se reconoce la necesidad *"de volver a examinar si el actual marco legal que regula el acceso a las comunicaciones privadas sigue siendo adecuado"*[39].

b) Los servicios de inteligencia y su regulación en Suecia

Investigaciones llevadas a cabo por periodistas y expertos apuntan a Suecia como un "socio" cada vez más importante de la red de inteligencia global, debido a sus numerosas relaciones con los Estados Unidos. La relación sueco-estadounidense radica en el interés mutuo. Gracias a esta alianza Suecia puede posicionarse en la "red de inteligencia global" como se constata con el Acuerdo UKUSA[40] que es una alianza de nacionales con el propósito de recolectar información de inteligencia al servicio del sistema de motorización ECHELON. Simultáneamente, los Estados Unidos consiguen un gran aliado desde un punto de vista geopolítico, pues les proporciona información proveniente de los Estados bálticos y sobretodo de Rusia.

Informes muestran como la agencia de inteligencia sueca (en adelante, FRA) recoge información a partir de cables de fibra óptica que cruzan las fronteras suecas desde los Estados bálticos y desde Rusia, almacenando (en la base de datos *"Titan"* por un período de 18 meses) y enviando la información hacia los Estados Unidos[41]. Así el 5 de diciembre de 2013 *Sveriges Television* informó que la FRA realizó, en nombre de la NSA, operaciones de vigilancia clandestinas a la política interna de Rusia. *Sveriges Television* reveló extractos de la NSA en una reunión con altos cargos de la FRA agradeciéndoles su colaboración[42].

39 Declaración de Rt. Hon. Sir Malcolm Rifkind (Presidente del Comité de Inteligencia y Seguridad del Parlamento británico) *"Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme"*, p.2, 17 de julio 2013.

40 Tratado de seguridad entre Reino unido, Estados Unidos, Australia, Canadá y Nueva Zelanda formada en 1946, también conocido como el Acuerdo UKUSA. Suecia firmó el Acuerdo UKUSA, de forma secreta, en 1954 de acuerdo con la prensa sueca : VINTHAGEN SIMPSON Peter *"Cold War treaty confirms Sweden was not neutral"*.

41 KLAMBERG Mark *"FRA and the European Convention on Human Rights"*.

42 STRUWE Filip y SVENSSON Anna *"SVT avslöjar: USA hyllar FRA:s ryss-spionage"*.

Desde un punto de vista jurídico, hasta 2009 la FRA solo podía obtener información a partir de las comunicaciones inalámbricas, incluyendo las señales de teléfonos móviles y de Internet. Pero debido a la gran cantidad de comunicaciones que se han realizado por cable y a la necesidad de adaptación del marco legal a las nuevas formas de amenaza internacional, se elaboró un proyecto de ley, conocido como "FRA lagen" (La Ley FRA)[43], que proponía modificaciones legislativas permitiendo que la FRA pudiera supervisar tanto las comunicaciones inalámbricas como por cable. El *Riksdag* (la asamblea legislativa sueca) aprobó el 18 de junio de 2008 el proyecto de ley, el cual entró en vigor el 1 de enero de 2009. Pero debido a la presión social FRA lagen tuvo que ser modificada dando lugar a un marco legislativo[44] que obligaba al servicio de inteligencia sueco a obtener autorizaciones legales por el Tribunal de Defensa e Inteligencia sueco (en adelante, UNDOM) para la interceptación de comunicaciones internas e impone límites en el almacenamiento de dicha información. Sin embargo, en el propio marco normativo se prevén excepciones a la obtención de las autorizaciones legales; autorizaciones legales que no son limitadas a personas específicas.

Ahora bien, una vez que esos datos son obtenidos, la legislación sueca permite transferir masivamente los datos a servicios de inteligencia extranjeros, requiriendo solo la autorización del gobierno[45]. Es a través de este mecanismo que las autoridades suecas han intercambiado grandes cantidades de información con los Estados Unidos y con los Estados bálticos. Si bien las autoridades suecas contribuyen de una forma importante con los *"Five Eyes"* enviando grandes cantidades de datos, inversamente FRA ha podido obtener datos de

43 Proyecto de Ley 2006/07:63 presentado por el Ministerio de Defensa sueco al Parlamento de Estocolmo, 8 de marzo 2007, en Suecia.

44 *Lag (2008:707) om signalspaning i försvarsunderrättelseverksamhet* (Ley 2008:707 sobre señales de inteligencia en las operaciones de defensa nacional), 10 de julio 2008, en Suecia; *Lag (2009:966) om Försvarsunderrättelsedomstol* (Ley 2009:966 sobre el Tribunal de Defensa e Inteligencia), 15 de octubre 2009, en Suecia; *Förordning (2009:968) med instruktion för Försvarsunderrättelsedomstolen* (Ordenanza con las instrucciones para el Tribunal de Defensa e Inteligencia), 15 de octubre 2009, en Suecia.

45 Ley 2008:707 sobre señales de inteligencia en las operaciones de defensa nacional, sección 9, 10 de julio 2008, en Suecia.

comunicaciones internas – sin la necesidad de obtener una autorización legal – a partir de las interceptaciones realizadas por agencias de los Estados bálticos[46].

La Opinión de la Comisión Europea del 10 de abril de 2014 sobre la vigilancia de las comunicaciones electrónicas[47], advierte que solo cuatro Estados miembros de la UE[48] contienen leyes nacionales de protección de datos que despliegan, en principio, la misma supervisión sobre los servicios de inteligencia que sobre cualquier otro controlador de datos. De entre estos cuatro Estados, se encuentra Suecia que cuenta con el servicio de Inspección Estatal de Inteligencia y Defensa (en adelante, SIUN)[49], compuesto de miembros del Gobierno y de partidos políticos de la oposición. Sin embargo, académicos expertos han criticado los grandes obstáculos que encuentra este sistema de control, como el Dr.Klamberg que pone de relevancia la falta de imparcialidad de sus miembros *"Todas estas instituciones [SIUN y UNDOM] están bajo un estricto control del Gobierno (...) Los miembros del SIUN representan diferentes partidos políticos pero son designados por el Gobierno y trabajan para el Gobierno. La mayoría de los miembros del SIUN son ex parlamentarios (...)*[50].

c) Los servicios de inteligencia y su regulación en Francia

Desde 2008, Francia ha estado continuamente mejorando su estructura para adaptarla a los métodos de obtención masiva de datos, mediante un aumento en las capacidades de la Dirección General para la Seguridad Externa (en adelante, DGSE). La DGSE intercepta y almacena, usando un "super ordenador", metadatos de emails, de mensajes de texto y de las facturas de móvil. Respecto a los datos,

46 KLEJA Monica *"FRA:s metoder granskas efter ny avlyssningsskandal"*.
47 GRUPO DE TRABAJO DEL ARTÍCULO 29 *"Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes"*, p.10.
48 Bulgaria, Hungría, Eslovenia, Suecia.
49 *Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelse verksamheten* (Ordenanza 2009:969 con las instrucciones para la inspección de las operaciones de inteligencia de defensa), 15 de octubre 2009, en Suecia.
50 KLAMBERG Mark "*European laws governing metadata collection and how it compares with U.S. Law on the subjetct"*.

éstos son interceptados y almacenados por estaciones de satélite y por cables submarinos de fibra óptica. De este modo Francia se sitúa en el quinto puesto en la obtención de metadatos (después de los Estados Unidos, Reino Unido, Israel y China) y en el segundo Estado, a nivel europeo, que más información procesa (tras Reino Unido).

Desde el año 2008, Francia ha desarrollado un importante dispositivo de interceptación de flujos de Internet (20 unidades de interceptación ha sido instaladas, como estaciones satélites y cables de fibra óptica submarinos), orientado principalmente al almacenamiento de metadatos, pues los servicios de inteligencia ya no buscan el contenido de los mensajes, sino su continente; es más interesante saber quién habla y a quién, que grabar lo que dicen. De este modo la DGSE es *"probablemente el centro informático más grande de Europa después de los ingleses"*, capaz de gestionar decenas de millones de gigabytes; *"el calor que desprenden los ordenadores consigue calentar los edificios de la DGSE..."*[51].

En Francia, el Código de la Seguridad Interior[52] creado en 2012 reagrupa todas las leyes relativas a la seguridad nacional. El Título IV del Libro II regula de forma exhaustiva las condiciones en las que la DGSE puede realizar interceptaciones, exigiendo una autorización escrita y motivada – válida por una duración máxima de 4 meses – del Primer Ministro, previa proposición por escrito del Ministro de Interior o del Ministro de Defensa o del Ministro encargado de las aduanas. El número máximo de interceptaciones susceptibles de ser realizadas simultáneamente es fijado por una orden del Primer ministro; decisión que debe ser puesta en conocimiento de la Comisión nacional de control de interceptaciones de seguridad. Las grabaciones han de ser destruidas a la expiración de un plazo de 10 días a partir de la fecha en que ha sido efectuada. En cuanto a las transcripciones de interceptaciones, éstas deben ser destruidas desde que su conservación no es indispensable para la realización de los objetivos.

51 FOLLOROU Jacques y JOHANNÈS Franck *"Révélations sur le Big Brother français"*.
52 *Code de la Sécurité Intérieure* (Código de la Seguridad Interior), 1 de mayo 2012, en Francia.

Ahora bien, existe un gran vacío legal pues no se regula ni la obtención y tratamiento de los metadatos, ni su almacenamiento masivo por la DGSE y posterior puesta en común a otros organismos. De este modo todo el dispositivo de la DGSE no es ilegal sino "alegal", como afirma uno de los jefes de una agencia de inteligencia *"Desde hace años estamos enmarcados en una autorización virtual y cada agencia se satisface ampliamente de esta libertad permitida gracias al flujo jurídico que existe alrededor de los metadatos"*[53].

El principal órgano responsable de la supervisión de las interceptaciones en Francia es, la Comisión Nacional de Intercepciones de Seguridad (en adelante, CNCIS). El CNCIS tiene la misión de ejercer un control, a priori, sobre las autorizaciones para realizar interceptaciones que concede el Primer ministro pues éste último tiene la obligación legal de informar, en un plazo máximo de 48 horas, al CNCIS. No obstante, el CNCIS tiene un limitado poder porque si considera que dicha autorización no respeta los principios de proporcionalidad, etc. entonces puede *"realizar una recomendación al Primer ministro tendente a que dicha interceptación sea interrumpida"*[54]. En otras palabras, el Primer ministro tiene la obligación de consultar al CNCIS pero las decisiones de este órgano no son vinculantes.

\J

Aunque ya había rumores sobre la existencia de alguno de estos sistemas de vigilancia, lo cierto es que los detalles sobre como funcionaban salieron a la luz a partir de las revelaciones de Edward Snowden. Sistemáticamente los gobiernos han justificado la existencia de esta vigilancia masiva por motivos de seguridad nacional. De ahí la importancia de los atentados del 11-S (Nueva York), 11-M (Madrid) y 7-J (Londres), pues han sido y son el pretexto de una vigilancia que no conoce límites.

53 FOLLOROU Jacques y JOHANNÈS Franck *"Révélations sur le Big Brother français"* en Le Monde, 4 de julio 2013.

54 Artículo L243-8 del Título IV, Libro II del Código de Seguridad Interior, en Francia.

1.2.2. Una vigilancia que va más allá de las fronteras europeas

En términos generales la función principal de los centros de inteligencia es detectar potenciales amenazas a la seguridad nacional, incluyendo amenazas terroristas, a través del almacenamiento de datos mediante técnicas especiales de investigación como vigilancia secreta, interceptación de comunicaciones, etc. pero aún con la tecnología más avanzada les es imposible poder controlar todo. Los centros de inteligencia necesitan cooperar entre ellos mediante el intercambio información y, aún más, a nivel europeo, teniendo en cuenta los riesgos que ha implicado la libre circulación de mercancías, personas, servicios y capitales. Ahora bien, si este intercambio no se inscribe en un marco legal claro, preciso, con estrictos controles realizados por un órgano independiente, este flujo de información puede afectar a los derechos de los ciudadanos.

El artículo 2.1 del Protocolo adicional al Convenio nº108 del Consejo de Europa describe el flujo de datos transfronterizo como la transferencia de datos personales a un destinatario que está sujeto a una jurisdicción extranjera. El Convenio establece una libre circulación de los datos personales entre los Estados parte del Convenio (todos los Estados miembros de la UE y los Estados del Espacio Económico Europeo son parte), de tal modo que la legislación nacional no deberá limitar el intercambio de datos, salvo cuando exista una legislación específica para ciertos datos de carácter personal o cuando la transmisión tenga por efecto burlar la legislación nacional (artículo 12.3). En definitiva, los intercambios de información de los centros de inteligencia europeos estarán regulados por las respectivas legislaciones nacionales, independientemente de que dichos flujos se produzcan entre Estados miembros o hacia Estados terceros.

A nivel europeo, la Directiva 95/46/CE regula las transferencias a países terceros de datos personales, pero, como se ha visto anteriormente, el artículo 3.2 excluye del ámbito de aplicación de la Directiva las actividades de los centros de inteligencia, y por ende, los intercambios de información.

Del mismo modo, la Decisión Marco 2008/977/JAI[55] del Consejo de la UE, tampoco se aplicaría a los centros de inteligencia, porque la aplicabilidad de la Decisión queda limitada a garantizar la protección de datos en la cooperación transfronteriza entre las autoridades competentes que trabajan en el ámbito de la policía y justicia penal (artículo 2, letra h).

Tras los atentados de Madrid del 11 de marzo de 2004, la UE intensificó sus esfuerzos dirigidos a promover el intercambio rápido y eficaz de información e inteligencia entre los servicios de seguridad de los Estados miembros. Como resultado el Consejo de la UE adoptó la Decisión Marco 2006/960/JAI[56], también conocida como la "iniciativa sueca" que impone a los Estados miembros *"cuando lo permita su legislación nacional, y de conformidad con ella"* (artículo 1.6) facilitar información o inteligencia a los servicios de seguridad de los Estados miembros.

No obstante, esta obligación de facilitar información, siempre que la legislación nacional lo permita, puede ser exceptuada si *"perjudicaría intereses esenciales en materia de seguridad nacional (...) comprometería el éxito de una investigación en curso o la seguridad de las personas (...) sería claramente desproporcionado o irrelevante para el fin que persigue la solicitud"* (artículo 10). Como se puede apreciar, estos motivos de denegación dejan un amplio margen de discrecionalidad a las autoridades nacionales competentes de los Estados miembros ante un requerimiento de información. En realidad el objetivo no es obligar a los centros de inteligencia a intercambiar información, sino simplemente a introducir en las relaciones entre los servicios de inteligencia de los Estado miembros el principio de disponibilidad. Se trata de evitar que el suministro de información se supedite a la obtención de una aprobación o autorización judicial cuando el servicio de seguridad competente requerido habría podido acceder sin

55 Decisión marco 2008/977/JAI, *relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal,* del Consejo de la Unión Europea, 27 de noviembre 2008.

56 Decisión Marco 2006/960/JAI, *sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea,* del Consejo de la Unión Europea, 18 de diciembre 2006.

aprobación o autorización judicial.

En consecuencia, la transferencia de datos de los servicios de inteligencia está integralmente regulada por las legislaciones nacionales, lo que da lugar a dos problemas principales. Por una parte, las legislaciones de los Estados miembros no suelen tener en cuenta los actos de sus servicios de inteligencia que se enmarcan dentro de los acuerdos de cooperación con otros centros extranjeros, porque estos acuerdos tienen una gran connotación política y se inscriben en el contexto de las relaciones internacionales entre los Estados. Por otra parte, en la mayoría de los Estados miembros, la legislación nacional no impone ninguna obligación a los servicios de inteligencia que tienda a asegurar que las informaciones han sido obtenidas sin vulnerar los derechos fundamentales de los ciudadanos[57]. Precisamente son estos dos "puntos débiles" en las legislaciones nacionales los que han permitido que los servicios de inteligencia, basándose en la cooperación e intercambio de información con otros centros, hayan podido obtener información de sus propios ciudadanos sin necesidad de cumplir con lo que dispone la ley.

A partir de las revelaciones de Edward Snowden parece que la concepción que ha imperado desde la Guerra fría que asocia los servicios de inteligencia con el secretismo y con un terreno de actuación marcado por la imprecisión sigue siendo real, lo que constituye un lastre en términos de apoyo social. Esta vigilancia masiva ha sido presentada como un *"friendly eye in the sky"* que cuida y previene. El problema es que a falta de regulación hay poca distancia entre un *"friendly eye"* y un Estado totalitario y omnipresente que todo lo ve. En los Estados de la UE, esta nueva noción de seguridad basada en las soluciones tecnológicas para vigilar, controlar y recopilar información privada, ha hecho que los servicios de inteligencia se viesen inmersos en un proceso de deslegitimación que solo podrá ser frenado con el establecimiento de una regulación.

57 SCHEININ Martin *"Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/10/3)"* p.16.

II. ¿Hacia una regulación europea de los servicios de inteligencia?

El derecho a la protección de datos no consigue abarcar todo lo que implican las misiones de los servicios de inteligencia – la seguridad nacional –. Del mismo modo, las legislaciones nacionales se encuentran limitadas para regular las actuaciones de los servicios de inteligencia y sus relaciones con otros servicios de seguridad extranjeros. La única solución parece evidente: establecer una regulación de los servicios de inteligencia de los Estados miembros a nivel europeo, pero ¿Es realmente posible? En esta sección se analizarán los obstáculos jurídicos que impiden a la UE legislar en el ámbito de los servicios de inteligencia. Después, se contemplara la posibilidad de un marco legal que establezca a EU INTCEN como un centro de inteligencia europeo.

2.1. Los obstáculos en la legislación de la Unión Europea

2.1.1. Una materia que escapa a las competencias de la Unión Europea

La configuración de la seguridad interior de la UE es el producto de un proceso que comenzó en la década de 1979 cuando se inició una colaboración informal entre representantes de los gobiernos de los Estados miembros, centrada en la prevención y lucha contra la criminalidad organizada y el terrorismo, mediante reuniones periódicas de los ministros de Interior y Justicia, en presencia de un representante de la Comisión, que conformaron el llamado "Grupo de Trevi".

Con la articulación del sistema de Schengen – por su relevancia, nos referiremos al "acervo de Schengen"[58] – esta cooperación informal se reveló insuficiente para

58 El "acervo de Schengen" está compuesto por dos Tratados (el *Acuerdo de supresión gradual de las fronteras interiores,* firmado por Alemania, Francia, Bélgica, los Países Bajos y Luxemburgo, 14 de junio 1985 y el *Convenio de aplicación del Acuerdo de Schengen,* firmado por Alemania, Francia, Bélgica, los Países Bajos y Luxemburgo, 19 de junio 1990) y por los actos y decisiones que en virtud de los mismos se han adoptado.

responder a las necesidades de seguridad de los ciudadanos europeos. En consecuencia, se incluyó en el Tratado de la Unión Europea (en adelante, TUE)[59] la denominada *"Cooperación en asuntos de justicia e interior"* que se configuró como "tercer pilar" con un marcado carácter de cooperación intergubernamental que incluía medidas que abarcaban desde el asilo y el control de fronteras a la lucha contra el fraude o la cooperación policial.

En 1997, con el Tratado de Amsterdam[60], se creo un *"Espacio de Libertad, Seguridad y Justicia"* (en adelante, ELSJ), al incorporar el "acervo de Schengen" al marco jurídico de la UE. La aplicación concreta del ELSJ se ha ido plasmando de forma exhaustiva en los Programas de Tampere (1999-2004)[61], de La Haya (2005-2009)[62] y en el de Estocolmo (2010-2014)[63]. Desde un primer momento, el ELSJ persigue garantizar la ausencia de controles de las personas en las fronteras interiores y desarrollar una política común de asilo, inmigración y control de las fronteras exteriores, así como asegurar un nivel elevado de seguridad mediante la prevención de la delincuencia, la cooperación judicial y policial en materia penal y el reconocimiento mutuo de las resoluciones judiciales y extrajudiciales en materia civil.

No obstante, el paso decisivo lo dio el Tratado de Lisboa. Además de la fusión de las anteriores Unión Europea y Comunidades Europeas en una única unión Europea (artículo 1 TUE) a la que se le reconoce expresamente personalidad jurídica (artículo 47 TUE), la seguridad interior se convirtió en una competencia compartida entre la UE y los Estados miembros. A esto se añade que se ha fijado,

59 *Tratado de la Unión Europea,* firmado por los representantes de los Estados miembros de la Unión Europea, 7 de febrero 1991, en Maastricht.

60 *Tratado de Amsterdam por el que se modifican el Tratado de la Unión Europea, Los Tratados constitutivos de las Comunidades Europeas y determinados actos conexos,* firmado por los representantes de los Estados miembros de la Unión Europea, 2 octubre 1997, en Amsterdam.

61 Conclusiones del Consejo Europeo de Tampere, 15 y 16 de octubre 1999.

62 COMISIÓN EUROPEA *"COM(2005)184 final. Comunicación de la Comisión al Consejo y al Parlamento Europeo.- Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia"* 10 de mayo 2005.

63 COMISIÓN EUROPEA *"COM(2009)262 final. Comunicación de la Comisión al Consejo y al Parlamento Europeo.- Programa de Estocolmo: Una Europa abierta y segura que sirva y proteja al ciudadano",* 10 de junio 2009.

en el artículo 39 del TUE, el respeto de las normas sobre protección de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la política exterior y seguridad común. Entonces, potencialmente, la UE tiene vocación a actuar en el escenario de la seguridad interior pero el propio Tratado de Lisboa ha introducido dos obstáculos.

El primero se encuentra en el artículo 72 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) que establece que los principales responsables de la seguridad pública y del mantenimiento del orden público son los Estados miembros.

El segundo obstáculo – que resulta de una petición de los británicos y quizás también de otros Estados miembros – es el artículo 4.2 del TUE que establece que *"(...) En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro"*. El alcance de este artículo se explicita en el artículo 73 del TFUE que precisa *"Los Estados miembros tendrán la posibilidad de organizar entre ellos y bajo su responsabilidad formas de cooperación y coordinación en la medida en que lo estimen apropiado, entre los servicios competentes de sus administraciones responsables de velar por la seguridad nacional"*. Aunque a primera vista parece ilógico que un tratado fundado en el principio atribución de competencias enuncie lo que los Estados pueden hacer en el marco de sus competencias respectivas, detrás de este artículo se entrevé la voluntad de hacer una Europa más dinámica en materia de seguridad nacional.

Sin embargo, los Estados miembros son especialmente reticentes a perder soberanía en el ámbito de la defensa y seguridad nacional. A lo largo del TUE se aprecia la insistencia por dejar claro que las competencias no atribuidas a la UE corresponden a los Estados miembros. El artículo 4.1 del TUE establece que *"(...) toda competencia no atribuida a la Unión en los Tratados corresponde a los Estados miembros (...)"* e inmediatamente después, en el artículo 5 del TUE en el

que, tras dejar también claro en su primer apartado que el sistema se rige por el principio de atribución expresa de competencia, vuelve a insistir en el apartado segundo al regular el principio de subsidiariedad que *"(...) Toda competencia no atribuida a la Unión en los Tratados corresponde a los Estados miembros (...)"*.

2.1.2. Una materia que escapa a un control jurisdiccional europeo

Desde su creación en 1952[64], el TJUE tiene por misión garantizar la aplicación e interpretación uniforme del Derecho de la UE. En el marco de esta misión, el TJUE controla la legalidad de los actos de las instituciones de la UE y de los Estados miembros – a través del recurso por incumplimiento, recurso de anulación y recurso por omisión– e interpreta el Derecho de la UE a solicitud de los jueces nacionales – mediante el mecanismo de la cuestión prejudicial –. Es el máximo intérprete del derecho de la UE; Derecho que a su vez legitima y delimita su competencia, ya que el TJUE no puede pronunciarse sobre cuestiones que escapan al ámbito de aplicación del Derecho de la UE. En consecuencia, el TJUE no puede tratar un asunto relativo a la actuación de un centro de inteligencia pues, como se ha mencionado anteriormente, esta competencia pertenece a los Estados miembros.

Recientemente, fue sometido a la Corte Suprema de Irlanda un litigio[65] que cuestiona la compatibilidad de las actuaciones de la sede en Europa de la red social Facebook con la Carta. El caso fue iniciado por Maximillian Schrems, un estudiante de derecho austriaco, que realizó el 25 de junio de 2013 una queja al Comisario irlandés de Protección de Datos acerca de la transferencia masiva de datos de los usuarios europeos de Facebook a la NSA a través del programa

64 *Tratado constitutivo de la Comunidad Europea del Carbón y del Acero* (CECA)*,* firmando por Francia, Alemania occidental, Italia, Luxemburgo, Bélgica y los Países Bajos, 18 de abril 1951, en París. El Tratado CECA expiró en 2002, pero sus instituciones quedaron integradas en la Comunidad Europea constituida por el Tratado de la Unión Europea.

65 Sentencia de la Corte Suprema de Irlanda 18 de junio 2014 (2013 765 JR), caso *Maximillian Schrems* c. *Data Protection Commissioner.*

PRISM, sin necesidad de una orden legal. El Comisario de Protección de Datos rechazó proceder a la investigación argumentando que la transferencia de datos de Facebook entraba dentro de los términos de un acuerdo de intercambio de datos entre la Unión Europea y los Estados Unidos conocido como *"Safe Harbor"* ("Acuerdo puerto seguro"); Acuerdo que había sido declarado compatible con la Directiva 95/46/CE por la Comisión Europea y en consecuencia, no había nada que investigar a no ser que Maximillian Schrems probara que la NSA había accedido a sus propios datos.

En realidad Safe Harbor no es un conjunto de disposiciones jurídicas sino un código de conducta redactado entre la UE y los Estados Unidos para las empresas estadounidenses. La adhesión al régimen se obtiene mediante un compromiso voluntario declarado ante el Departamento de Comercio de Estados Unidos y se documenta en una lista publicada por dicho departamento. Para asegurar la eficacia de la protección de datos, las empresas estadounidenses que adhieran a Safe Harbor estarán bajo la supervisión de la Comisión Federal de Comercio de los Estados Unidos. La adhesión de las empresas estadounidenses a Safe Harbor les otorga grandes ventajas en lo que respecta la Directiva 95/46/CE. Tal y como se ha mencionado anteriormente, la Directiva establece (artículo 25.1) que solo pueden transferir datos personales de los Estados miembros de la UE a otros países terceros en la medida en que tales países garanticen un nivel de protección adecuado, no obstante también se prevé (artículo 25.6) que la Comisión Europea es competente para valorar el nivel de protección de datos en los países extranjeros mediante decisiones – "decisiones de adecuación" – sobre el carácter adecuado de la protección y realizar consultas sobre la evaluación al Grupo de Trabajo del artículo 29. El 26 de julio de 2000, la Comisión Europea adoptó la Decisión 2000/520/CE[66] (en lo sucesivo denominada, "la Decisión Safe Harbor") en la que reconoce que Safe Harbor ofrece un nivel de protección adecuado a fines de transferencia de datos personales desde la UE.

66 Decisión 2000/520/CE, *"sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos de América",* adoptada por la Comisión Europea con arreglo a la Directiva 95/46/CE, 26 de julio 2000.

Frente al rechazo de iniciar la investigación, Maximillian Schrems acudió a la Corte Suprema de Irlanda con el fin de obtener un control jurisdiccional sobre la decisión del Comisario de Protección de Datos. La Corte Suprema de Irlanda tras subrayar que el asunto no versa ni sobre la validez de la Directiva 95/46/CE, ni sobre la Decisión Safe Harbor[67] y que el Maximillian Schrems no estaba obligado a demostrar que sus propios datos habían sido espiados con el fin de presentar una queja[68], planteó dos cuestiones prejudiciales al Tribunal de Justicia de la Unión Europea[69].

La primera de ellas consiste en saber si el Comisario de Protección de Datos de Irlanda, frente a una queja en la que se afirma que se están transmitiendo datos personales a un tercer país donde no se prevé una protección adecuada de datos, está vinculado en términos absolutos por la Decisión Safe Harbor. La segunda cuestión planteada trata sobre si, a la luz de la evolución de los hechos que han tenido lugar desde que se publicó por primera vez la Decisión Safe Harbor[70], el Comisario de Protección de Datos de Irlanda tenía una facultad o un deber de iniciar de oficio una investigación sobre las transferencias de datos de Facebook hacia los Estados Unidos.

Respecto a la primera cuestión prejudicial, se puede tomar como referencia la sentencia dictada un mes antes por el TJUE en el marco de una petición prejudicial planteada por la Audiencia Nacional de España[71].

La demanda fue interpuesta en 2010 por un ciudadano español junto con la Agencia Española de Protección de Datos (en adelante, AEPD) contra Google

67 Sentencia de la Corte Suprema de Irlanda 18 junio 2014, §69.

68 Sentencia de la Corte Suprema de Irlanda 18 junio 2014, §45.

69 Petición de decisión prejudicial planteada por la Corte Suprema de Irlanda 25 de julio 2014 (asunto C-362/14), caso *Maximillian Schrems* c. *Data Protection Commissioner*.

70 Sentencia Corte Suprema de Irlanda 18 de junio 2014, *"(...) Hay, tal vez, mucho que decir a favor del argumento de que Safe Harbor se ha visto superado por los acontecimientos. Puede pensarse que las revelaciones de Snowden han puesto de manifiesto enormes agujeros en la práctica contemporánea de protección de datos de los Estados Unidos y la posterior entrada en vigor del Artículo 8 de la Carta sugiere que puede ser necesaria una re-evaluación en como deberían ser interpretadas en la práctica la Directiva de 1995 y la Decisión de 2000 (...)" §69.*

71 Sentencia TJUE 13 mayo 2014 (asunto C-131/12), caso *Google Spain S.L y Google Inc* c. *AEPD y el Sr.Costeja González*.

Spain S.L y Google Inc. El demandante consideraba que un aviso de subasta de su casa embargada que aparecía en los motores de búsqueda de Google infringía sus derechos de privacidad porque los procedimientos que le concernían ya habían sido completamente resueltos hace años y la referencia era completamente irrelevante. Se requería a Google Spain S.L y Google Inc. a eliminar los datos personales relativos a él, para que no aparezcan más en los motores de búsqueda.
En su sentencia del 13 de mayo de 2014, el TJUE declaró que respecto a la territorialidad del Derecho de la Unión Europea, incluso si el servidor físico de la una compañía de procesamiento de datos se localiza fuera de Europa, las reglas europeas se aplican al operadores de búsqueda si tiene una sucursal o un establecimiento subsidiario en un Estado miembro. En cuanto a la aplicabilidad de las normas europeas a un motor de búsqueda, el TJUE consideró que los motores de búsqueda son controladores de datos personales y en consecuencia se les aplican las leyes europeas de protección de datos y también el "derecho de olvido", que es el derecho de todo individuo a pedir a los motores de búsqueda la eliminación de *links* o enlaces con datos personales sobre ellos. Esto se aplica cuando la información es inexacta, inadecuada, irrelevante o excesiva para los propósitos del procesamiento de datos.

En consecuencia el TJUE declaró que Google estaba sometido a las normas europeas de protección de datos y sin embargo, Google es una empresa estadounidense adherida Safe Harbor desde el 15 de octubre de 2015. El hecho de que Google estuviese adherido a Safe Harbor no fue un dato que impidiera la aplicación de las leyes europeas de protección de datos. Del mismo modo, tampoco se consideró que la AEPD – el equivalente en España del Comisario de Protección de Datos de Irlanda – estuviese de alguna forma vinculada con la Decisión Safe Harbor de la Comisión Europea. Siguiendo esta línea jurisprudencial, el hecho de que Facebook tenga el autocertificado de Safe Harbor no impide al Comisario de Protección de Datos de Irlanda iniciar una investigación sobre las actuaciones de Facebook.

El litigio no está resuelto aún – se prevé una respuesta a las cuestiones prejudiciales en 2016 – pero tras las deficiencias de Safe Harbor, la propia Comisión Europea en una comunicación al Parlamento Europeo y al Consejo de la UE[72], ha expresado su inquietud: *"(...) las informaciones divulgadas recientemente sobre los programas de vigilancia estadounidenses, que plantea nuevas cuestiones acerca del nivel de protección que se supone debe garantizar el marco de puerto seguro"*. El problema no reside tanto en el modo en que las empresas estadounidenses aplican Safe Harbor sino en *"la formulación excesivamente general de los principios, así como la fuerte dependencia de la autocertificación y la autorregulación"*. A raíz de las revelaciones sobre los programas, algunas de las autoridades de protección de datos alemanas fueron especialmente rigurosas y *"han pedido a las empresas que transfieran datos personales a proveedores estadounidenses que les comuniquen si dichos proveedores impiden a la Agencia Nacional de Seguridad estadounidense el acceso a los datos, y cómo lo hacen"*.

Sin embargo, aún con una reforma eficaz de Safe Harbor, el problema persistiría pues la filial de Facebook en Europa – Facebook Ireland Ltd. – podría transmitir dichos datos al GCHQ, el cual a su vez los transmitiría a la NSA – igualmente a través del programa PRISM – y todo ello sin que el TJUE tuviera competencia para pronunciarse sobre el litigio. Aún estando vulnerado el derecho europeo a la protección de datos, al estar involucrado un centro de inteligencia de un Estado miembro, el TJUE no tiene competencia.

72 COMISIÓN EUROPEA *"COM(2013) 847 final. Comunicación de la* Comisión al Parlamento Europeo y al Consejo de la Unión Europea *sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE"*, pp.3-6.

2.2. EU INTCEN, como un posible punto de partida

2.2.1. Un marco legal indeterminado

El Centro de Análisis de Inteligencia de la Unión Europea (en adelante, EU INTCEN) es la actual denominación que se da a la única institución europea encargada de proporcionar análisis de inteligencia, alerta temprana y consciencia situacional. Sus orígenes se remontan a la Unión Europea Occidental, una organización de defensa formada por los Estados miembros de la Unión Europea y los miembros europeos de la Organización del Tratado del Atlántico Norte que fue oficialmente disuelta en junio de 2011.

No fue hasta el año 2000 que la entidad, bajo el nombre de Centro de Situación Conjunto (en adelante, SITCEN), se dotó de autonomía para asistir a la UE en las situaciones de crisis. Dicha transformación fue el resultado de la decisión administrativa de Javier Solana, primer Alto Representante de la Unión para la Política Común de Seguridad y Defensa. A partir de esta decisión, SITCEN fue adscrita a la Oficina del Alto Representante y, por consiguiente paso a ser parte integrante de la Secretaría General del Consejo de la UE. Sin embargo, la legitimidad de esta transformación ha sido puesta en duda debido a que es el resultado de una decisión individual del Alto Representante, sin que el Consejo de la UE haya adoptado formalmente ningún acto legal[73].

En 2002, SITCEN no era una estructura que trabajaba exclusivamente sobre información proveniente de fuentes accesibles al público, sino que también intercambiaba inteligencia con los servicios de inteligencia de los Estados miembros.

Cinco años después, en 2007, el centro era capaz de analizar situaciones fuera de la UE gracias al establecimiento de la Capacidad de Análisis de Inteligencia Único que permitía la entrada de inteligencia necesarias para responder a situaciones de crisis y evaluar situaciones situadas fuera de la UE.

Finalmente, en 2010, SITCEN fue transferido al Servicio Europeo de Acción

73 VAN BUUREN Jelle *"The Secret Truth. The EU Joint Situation Centre"*.

Exterior (en adelante, EEAS)[74], convirtiéndose en una estructura, bajo la responsabilidad del Alto Representante, que asiste a la red mundial de delegaciones de la UE y a las operaciones de la PCSD.

Ahora bien, la Decisión 2010/427/EU del Consejo de la UE por la que se establece el EEAS no contiene disposiciones que expresamente constituyan a SITCEN. Tampoco existe ningún otro documento que constituya formalmente a SITCEN. Solo se prevé en el anexo de la Decisión 2010/427/EU que el personal y las funciones de SITCEN serán transferidas *"en bloque"* al EEAS, salvo el personal que asista en la Autoridad de Acreditación de Seguridad.

Actualmente, EU INTCEN – la nueva denominación de SITCEN tras la remodelación estructural de marzo de 2012 en el EEAS – sigue expandiendo sus poderes y fortaleciendo su estructura gracias al respaldo político de la UE y de las instituciones de los Estados miembros, pero sin tener ningún texto legal de base. Así lo declaró Ilkka Salmi, el actual director de EU INTCEN y antiguo director del centro de inteligencia finlandés: *"No hay ningún tipo de documento que establezca claramente INTCEN (...) diciendo: este es el nombre, su función, el alcance de sus actividades, lo que pueden hacer. Este tipo de documento no existe"*[75]. En su lugar, solo existe la Decisión del Consejo de la UE de 26 de julio de 2010 en la que se afirma que SITCEN – el antecesor de EU INTCEN – forma parte del EEAS y una ficha técnica[76] proveniente del EEAS donde se explica escuetamente en qué consiste EU INTCEN.

74 Decisión 2010/427/EU, *por la que se establece la organización y el funcionamiento del Servicio Europeo de Acción Exterior,* del Consejo de la Unión Europea, 26 de julio 2010.
75 KRISTOF Clerix *"Ilkka Salmi, the EU's spymaster",* p.6.
76 EEAS *"Fact Sheet EU INTCEN"*.

2.2.2. Un mandato opaco

A la diferencia de los servicios de inteligencia de los Estados miembros, EU INTCEN no tiene capacidad operacional en el terreno. EU INTCEN es un centro que proporciona análisis estratégicos de inteligencia al Alto Representante de la UE – actualmente Federica Mogherini –, al EEAS y a los Estados miembros. Mediante el seguimiento y evaluación de los acontecimientos internacionales, centrándose especialmente en las zonas geográficas sensibles, el terrorismo, la proliferación de armas de destrucción masivas y otras amenazas globales EU INTCEN *"intenta apoyar al EEAS en la formulación de sus políticas proporcionando el componente de inteligencia en el proceso"*[77].

Teniendo en cuenta la naturaleza de las funciones y documentos que produce EU INTCEN es comprensible que se intente ocultar el trabajo que llevan a cabo, pero el gran vacío legal que envuelve al centro implica una ausencia de transparencia que ha dado lugar a malentendidos, incluso por parte de algunos europarlamentarios que han llegado a afirmar que *"EU SITCEN es el equivalente europeo a la CIA"*[78].

Esta falta de transparencia deriva también del limitado acceso que tienen los europarlamentarios a los documentos que provienen de EU INTCEN. Solo tienen acceso a los documentos algunos europarlamentarios en situaciones en las que dicha información es necesaria, por ejemplo si están trabajando en un comité que trata con asuntos de seguridad y defensa y necesitan información sobre un tema determinado. A esto se añade que dichos europarlamentarios no están habilitados para compartir sus hallazgos con otros europarlamentarios.

Todo ello impide un mínimo control parlamentario y ha creado gran desconfianza sobre las actuaciones de EU INTCEN. De hecho, tras ser vistos en 2012 en Trípoli y Bengasi (Libia) a dos funcionarios de EU INTCEN, muchos europarlamentarios

77 KRISTOF Clerix *"Ilkka Salmi, the EU's spymaster",* p.1.

78 WILLS Aidan, VERMEULEN Mathias, BORN Hans, SCHEININ Martin, WIEBUSCH Micha *"Parliament Oversight of Security and Intelligence agencies in the European Union",* p.56.

se alarmaron y no comprendían lo que estaba ocurriendo, como por ejemplo la europarlamentaria británica, Sarah Ludford, miembro del Grupo de la Alianza de los Liberales y Demócratas por Europa que declaró lo siguiente en el canal de televisión Europarl TV: *"no está del todo claro por qué están poniendo a gente en el terreno. ¿Pero esto no podría poner en peligro la misión al estar expandiendo sus poderes originales? Creo que debemos estar atentos a esto"*. Posteriormente, Ilkka Salmi aclaró cuales eran las actividades de EU INTCEN y declaró que se trataba de *"un miembro del personal técnico – no un analista – que estaba ayudando con un satélite"* aunque también precisó que el personal de EU INTCEN hace visitas, incluso fuera de la UE, para obtener información sobre las regiones que están tratando de evaluar[79]. Probablemente si se hubiesen establecido bases legales que definan lo que EU INTCEN puede hacer y como debe hacerlo no hubiesen sido necesarias tantas aclaraciones. Aunque peor es el hecho de que los europarlamentarios pensaran que EU INTCEN estaba llevando a cabo operaciones de inteligencia sobre el terreno, pues esto refleja la desconfianza que existe hacia este centro.

Frente a los atentados en Paris, el pasado 7 de enero, la europarlamentaria neerlandesa miembro del Grupo de la Alianza de los Liberales y Demócratas por Europa, Sophie Int'Veld, puso de relieve la necesidad de convertir a EU INTCEN en una agencia de inteligencia con su propio tratado constitutivo, marco legislativo y previsiones sobre un control democrático. Asimismo, el primer ministro italiano respaldó la idea de una agencia de inteligencia europea. En cambio, Ilkka Salmi considera que *"hay suficientes bases legales para las actividades de EU INTCEN. El EEAS ha sido establecido por un texto legal que hace mención a EU INTCEN (...)"*[80]. Del mismo modo, la portavoz de la Comisión Europea, Natasha Bertuad, respondió con un tajante "No." ante la posibilidad de que EU INTCEN se convirtiese en una agencia de inteligencia[81]. Según la Comisión Europea los esfuerzos se han de centrar en mejorar la

79 KRISTOF Clerix *"Ilkka Salmi, the EU's spymaster",* p.4.
80 KRISTOF Clerix *"Ilkka Salmi, the EU's spymaster",* p.6.
81 NIELSEN Nikolaj *"No plan for EU spy agency after Paris attacks"*.

coordinación entre EU INTCEN y los entes policiales y de inteligencia de los Estados miembros, pues el asalto en la sede del periódico *Charlie Hebdo* fue realizado por dos hermanos que ya eran conocidos por la policía. Se sabía que uno de ellos había sido entrenado en Yemen por al Quaeda, mientras que el otro había viajado a Siria el año pasado. Sin embargo, ¿deben los Estados miembros confiar en una estructura europea que carece de bases legales y cuyo mandato no es transparente?

Conclusiones

Los límites que encuentra el derecho europeo a la protección de datos en todo lo que afecta a los servicios de inteligencia de los Estados miembros ha cobrado más importancia que nunca. Desde hace una década, el gran desarrollo tecnológico ha hecho posible la obtención, el tratamiento y el intercambio de datos de manera masiva e indiscriminada y los servicios de inteligencia no han desperdiciado la ocasión para poner a su servicio esta sofisticada tecnología. La información se ha convertido en un valioso instrumento para poder ejercer una vigilancia que a penas conoce límites.

No obstante, a partir de las revelaciones de Edward Snowden, la opinión pública no solo ha cuestionado la eficacia del derecho europeo a la protección de datos, sino también la propia legitimidad los servicios de inteligencia, emergiendo así la posibilidad de establecer una regulación europea de los servicios de inteligencia pero, ¿es realmente posible una regulación de lo secreto? Sin duda, es necesario para proteger el derecho a la protección de datos, pero todavía no hay el respaldo político suficiente para cambiar las bases legales del Tratado de Lisboa y dotar a la UE de competencias en este ámbito. Ni siquiera existe la voluntad de dotar de un marco jurídico propio a una estructura europea que actualmente trabaja con inteligencia y que podría constituir un punto de conexión entre los distintos servicios de inteligencia de los Estados miembros y también el inicio de una regulación europea de los servicios de inteligencia.

Bibliografía

BOILLAT Philippe, KJAERUM Morten *Manual de legislación europea en materia de protección de datos*. Luxemburgo: Ed. Oficina de Publicaciones de la Unión Europea, 2014.

BOWCOTT Owen *"UK-US surveillance regime was unlawful for seven years"* en The Guardian, 6 de febrero 2015 [http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa].

BUZAN Barry *People, States & Fear: an agenda for international security studies in the post-cold war era.* Segunda edición. Colchester: Ed. ECPR Press, 2007.

COMISIÓN EUROPEA *"COM(2013) 847 final. 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"*, 27 de noviembre 2013 [http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf]

DE KERCHOVE Gilles *"L'Union européenne et le monde dans la luttle contre le térrorisme",* en : DONY Marianne, *La dimension externe de l'espace de liberté, de sécurité et de justice au lendemain de Lisbonne et de Stockholm: un bilan à mi-parcours,* Bruselas: Ed. Université de Bruxelles, 2012.

DÍAZ FERNÁNDEZ, Antonio Manuel *"La función de los servicios de inteligencia"*, en : DE CUETO Carlos y JORDÁN Javier (Coords), *Introducción a los Estudios de seguridad y defensa*, Granada: Ed. Linares, 2001.

DIDIER Bigo, CARRERA Sergio, HERNANZ Nicholas, JEANDESBOZ Julien, PARKIN Joanna, RAGAZZI Francesco, SCHERRER Amandine *"National programmes for mass surveillance of personal data in EU Member States and their compability with EU law",* estudio del Departamento de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo, 2013 [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf].

DIDIER Bigo, CARRERA Sergio, HERNANZ Nicholas, JEANDESBOZ Julien, PARKIN Joanna, RAGAZZI Francesco, SCHERRER Amandine *"UK surveillance: justice, freedom and security in the EU"* en Open Democracy, 14 de mayo 2014 [https://www.opendemocracy.net/can-europe-make-it/didier-bigo-sergio-carrera-nicholas-hernanz-julien-jeandesboz-joanna-parkin-fra-4].

EEAS *"Fact sheet EU INTCEN"*, 5 de febrero 2015 [http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf].

FOLLOROU Jacques y JOHANNES Franck *"Révélations sur le Big Brother français"* en Le Monde, 4 de julio 2013 [http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html].

GELLMAN Barton y SOLTANI Ashkan *"NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say"* en The Washington Post, 31 de octubre 2013 [http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html].

GRUPO DE TRABAJO DEL ARTÍCULO 29 (WP 215 819/14/EN) *"Opinion 04/2014 on suveillance of electronic communications for intelligence and national security purposes",* 10 de abril 2014 [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf].

HAYCOCK Ronald *"The Evolution of Canadian National Security Policy",* estudio del Centro para Estudios sobre Seguridad Nacional, en Canada, 1994.

KLAMBERG Mark *"European laws governing metadata collection and how it compares with U.S. Law on the subject"* en Lawfare, 29 de septiembre 2013 [http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection/].

KLAMBERG Mark *"FRA and the European Convention on Human Rights – A Paradigm Shift in Swedish Electronic Surveillance Law"* en: SCHARTAUM Dag Wiese (Ed.), *Overvåking i en rettstat in the series Nordisk årbok i rettsinformatikk*, Bergen: Ed. Fagforlaget, 2010, pp.96-134.

KLEJA Monica *"FRA:s metoder granskas efter ny avlyssningsskandal"* en NyTeknik, 27 de agosto 2008 [http://www.nyteknik.se/nyheter/it_telekom/internet/article248226.ece].

KRISTOF Clerix *"Ilkka Salmi, the EU's spymaster"* en Mondiaal Nieuws, 4 de marzo 2014 [http://www.mo.be/en/interview/ilkka-salmi-eu-s-007].

MACASKILL Ewen, BORGER Julian, HOPKINS Nick, DAVIES Nick y BALL James *"GCHQ taps fibre-optic cables for secret access to world's communications"* en The Guardian, 21 de junio 2013 [http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa].

MARTÍN MARTÍNEZ Mª Magdalena *"El espacio de Libertad, Seguridad y Justicia",* en : ALCAIDE FERNÁNDEZ Joaquín y CASADO RAIGÓN Rafael (Coords), *Curso de Derecho de la Unión Europea,* Madrid: Ed. Tecnos, 2011.

MARTÍN Y PÉREZ DE NANCLARES José y URREA CORRES Mariola *Tratado de Lisboa.* Madrid: Ed. Real Instituto Elcano & Marcial Pons, 2008.

NIELSEN Nikolaj *"No plan for EU spy agency after Paris attacks"* en EU Observer, 12 de enero 2015 [https://euobserver.com/justice/127175].

REBOLLO DELGADO Lucrecio *Vida privada y protección de datos en la Unión Europea.* Madrid: Ed. Dykinson S.L, 2008.

SCHEININ Martin *"Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/10/3)"* informe de la Asamblea General de las Naciones Unidas, 4 de febrero 2009 [http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/106/25/PDF/G0910625.pdf?OpenElement].

STRUWE Filip y SVENSSON Anna *"SVT avslöjar: USA hyllar FRA:s ryss-spionage",* en Svt Nyheter, 5 de diciembre 2013 [http://www.svt.se/nyheter/inrikes/fra-spionerar-pa-ryssland-at-usa].

VAN BUUREN Jelle *"The Secret Truth. The EU Joint Situation Centre"* informe del Instituto holandés Stichting Eurowatch, 2009 [http://www.statewatch.org/news/2009/aug/SitCen2009.pdf].

VINTHAGEN SIMPSON Peter *"Cold War treaty confirms Sweden was no neutra"* en The Local, 9 de diciembre 2013 [http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral].

WILLS Aidan, VERMEULEN Mathias, BORN Hans, SCHEININ Martin, WIEBUSCH Micha *"Parliament Oversight of Security and Intelligence agencies in the European Union",* estudio del Departamento de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo, 2011 [http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf].