FACULTAD DE DERECHO, UNIVERSIDAD PONTIFICIA COMILLAS

DERECHO A LA PRIVACIDAD VERSUS SEGURIDAD DEL ESTADO: LÍMITES EN LA LUCHA CONTRA EL TERRORISMO.

Autor: Ana María Alfonso Ramos
Tutor: Paula García Andrade

Madrid
Abril 2014


PONTIFICIA UNIVERSITAS COMILLENSIS
MATRITI

ÍNDICE

LISTADO DE ABREVIATURAS Y SIGLAS:

CEDH: Convenio Europeo de Derechos Humanos.

TEDH: Tribunal Europeo de Derechos Humanos.

TJUE: Tribunal de Justicia de la Unión Europea.

CDFUE: Carta de Derechos Fundamentales.

APEC: Foro de Cooperación Económica Asia-Pacífico.

OCDE: Organización para la Cooperación y el Desarrollo Económico.

EEUU: Estados Unidos de América.

UE: Unión Europea.

ONU: Organización de Naciones Unidas.

TUE: Tratado de la Unión Europea.

LIBE: Comité de Libertades Civiles, Justicia y Asuntos de Interior.

NSA: Agencia de Seguridad Americana.

GCHQ: Britain's Government Communications Headquarters.

SWIFT*: Society for Worldwide Interbank Financial Telecommunications*.

RESUMEN Y PALABRAS CLAVE:

Las cuestiones discutidas en el presente proyecto son las vulneraciones al derecho de la privacidad cometidas por la Agencia de Seguridad Nacional Americana (*en adelante,* NSA) junto con las agencias de espionaje europeas, las revelaciones de Edward Snowden y los Acuerdos logrados entre Estados Unidos y la Unión Europea. Se estudiará la protección jurídica de dicho derecho y se analizará jurisprudencia del Tribunal Europeo de Derechos Humanos (*en adelante*, TEDH) y de la Corte de Justicia de la Unión Europea (*en adelante*, TJUE). Se profundizará en las medidas adoptadas por la Unión Europea (*en adelante*, UE) y los Estados Unidos (*en adelante*, EEUU) para lograr soluciones jurídicas viables que acerquen posturas y consigan un equilibrio entre privacidad y seguridad.

Palabras clave: privacidad, límites, seguridad, CEDH, terrorismo, NSA, espionaje, agencias de seguridad, protección, transmisión de datos.

The issues discussed in this paper are privacy violations, which have been committed by the National Security Agency in cooperation with the European secret agencies. Moreover, the revelations of Edward Snowden and the agreements reached between the United States and the European Union are discussed. The legal protection of the human right to privacy will be studied in depth analyzing the jurisprudence of the European Court of Human Rights as well as the European Court of Justice to highlight the violations committed in the legal framework. As spying has been a new mean of acquiring private information, it will be discuss on the paper the proposals adopted by both the US and the EU in order to achieve viable legal solutions to bring positions together and thus accomplish the balance long sought between privacy and security.

Key words: *privacy, limitations, security, ECHR, terrorism, NSA, espionage, security agencies, protection and data transmission.*

INTRODUCCIÓN:

1. Definición de la cuestión objeto de investigación:

1.1 Interés de su tratamiento.

Al ser el derecho a la privacidad un derecho humano, se estudiará su vulneración por algunos Estados y nos centraremos sobre todo en cómo esta violación ha afectado a ciudadanos europeos.

La exposición abordará acontecimientos actuales y mantendrá un debate continuo entre el derecho humano de privacidad y el bien común de la seguridad. Se aportaran los comentarios, la jurisprudencia y la doctrina necesarios para una mejor comprensión del tema que permita llegar a unas conclusiones específicas.

Es interesante la elección de este tema por su total actualidad y su repercusión directa en el derecho de las personas a su vida privada sin injerencias arbitrarias como el espionaje estatal. Como contrapartida, se abordará la necesidad de garantizar la seguridad de los ciudadanos y Estados para luchar contra el terrorismo. El trabajo analiza el derecho a la privacidad de los ciudadanos como particulares y no la privacidad de los Estados como sujetos de Derecho Internacional Público. Por ello, las vulneraciones que explicamos en el trabajo afectan de primera línea a los ciudadanos como sujetos particulares. Además, la gran cantidad de estados implicados o cuyos intereses se ven afectados por este debate acrecienta todavía más la importancia de este asunto. Por último, el derecho humano a la privacidad se debate en conferencias internacionales y afecta principalmente a países miembros de la UE considerados más proteccionistas frente a los EEUU que adopta una postura más liberal.

1.2 Delimitación del marco temporal que será analizado.

El tema seleccionado es una cuestión abierta en pleno debate y negociación y se debe comenzar explicando las cuestiones más recientes: el espionaje cometido por la NSA y determinadas agencias europeas que salió a la luz el mes de junio de 2013 debido a las revelaciones públicas del ex contratista de dicha agencia, Edward Snowden. También se analizan los dos acuerdos relativos a la transmisión de datos entre la Unión Europea y los EEUU para tratar de llegar a una mayor protección a la privacidad, el Acuerdo de Puerto Seguro de 2006 y el Acuerdo SWIFT de 2010. No debemos olvidar que mencionamos sentencias de tribunales que son anteriores a dicho marco temporal para tomarlas como punto de referencia en el trabajo y poder analizar los elementos tanto de la privacidad y la seguridad. El momento temporal elegido para la conclusión del trabajo serán las últimas noticias de estos primeros meses de 2014 quedando abierto este debate a futuras conclusiones.

2. Objetivos perseguidos.

Este trabajo analiza los elementos del art. 8 del Convenio Europeo de Derechos Humanos (*en adelante*, CEDH) para verificar si las cuestiones fácticas mencionadas previamente suponen una vulneración a dicho artículo. El objetivo no es determinar si el derecho a la privacidad predomina sobre el bien de la seguridad o viceversa, sino llegar a la conclusión que la privacidad es un derecho humano que tiene que ser respetado a nivel internacional por su protección en la Declaración Universal de los Derechos Humanos (*en adelante*, DUDH), a nivel regional por los tratados existentes y en el ámbito nacional por las constituciones nacionales. Nos hemos centrado en la protección jurídica de dicho derecho en el marco europeo debido a las vulneraciones sufridas por los ciudadanos europeos en los últimos tiempos. Se destaca también que únicamente se permitirá interferir en la privacidad de los ciudadanos cuando se cumplan los límites del apartado segundo del art. 8 del CEDH y predomina la defensa de la seguridad.

3. Metodología y plan de trabajo.

En primer lugar nos ha parecido necesario comenzar por un capítulo preliminar que nos permite entrar en contacto con los temas más recientes que han supuesto una vulneración al derecho de la privacidad. Asimismo identificaremos los protagonistas principales, los EEUU y los Estados miembros de la UE.

El grueso del escrito se centrará en los capítulos posteriores desarrollando la fundamentación jurídica de dicho derecho y las limitaciones a la privacidad para garantizar la seguridad ciudadana. El capítulo primero comenzará explicando de forma teórica el concepto de privacidad para con posterioridad centrarse en la protección jurídica, que se recibe en el ámbito del Consejo de Europa y dentro de la Unión Europea. En ambos capítulos se estudian sentencias que han supuesto una vulneración a la privacidad y otras en las que se han cumplido los límites para luchar contra el terrorismo y garantizar la seguridad de los ciudadanos.

En las conclusiones se valorarán la efectividad de las sentencias mencionadas, así como se analizará cómo el espionaje y los nuevos medios de comunicación están suponiendo una vulneración a la privacidad. Se recogerán por último las posibles soluciones para evitar dichas vulneraciones fundamentales.

CAPÍTULO PRELIMINAR: CUESTIONES FUNDAMENTALES QUE AFECTAN AL DERECHO A LA PRIVACIDAD Y LA PROTECCIÓN PARA VELAR POR LA SEGURIDAD DEL ESTADO.

El avance progresivo de la ciencia y las tecnologías ha supuesto una injerencia en la esfera privada de las personas, violándose por tanto el derecho humano a la privacidad.

En este capítulo preliminar del trabajo intentamos exponer los casos más relevantes en los que se produce dicho enfrentamiento para poder analizar posteriormente la protección jurídica existente a nivel internacional y su protección en el marco jurídico europeo.

Analizamos en primer lugar el supuesto espionaje cometido por la NSA y el caso Snowden. Posteriormente, estudiamos los problemas que han surgido en los Acuerdos de protección de datos: el Acuerdo de Puerto Seguro y el Acuerdo *SWIFT*. Concluimos destacando la importancia actual del comercio electrónico.

1. Acontecimientos problemáticos y actuales que enfrentan la privacidad de los ciudadanos y la seguridad del Estado.

En este primer apartado explicamos el caso de espionaje más próximo en el tiempo, analizando cuáles han sido las vulneraciones al derecho de privacidad de las personas.

1.1 El espionaje realizado por la NSA junto con las revelaciones de Edward Snowden y las vulneraciones cometidas.

Una de las principales funciones de la NSA y de los servicios de espionaje extranjeros es la recopilación de información y de datos privados pertenecientes a los ciudadanos norteamericanos y extranjeros para evitar posibles amenazas terroristas.

La recopilación de información se produce principalmente desde el cambio geo-político y social que ha sufrido el mundo occidental desde los ataques terroristas del 11 de septiembre en Nueva York y del 11 de marzo en Madrid. Esto supuso en su día el incremento de la vigilancia a través de nuevos medios tecnológicos para evitar posibles amenazas a la seguridad de los Estados.[1] La creciente implantación de nuevos medios tecnológicos de vigilancia, seguimiento, observación o control generalizado de datos encarna un riesgo de limitación de los derechos propios de la esfera privada del individuo y crea una polémica latente en la sociedad democrática actual.

Esta cuestión se ha convertido en un tema controvertido a nivel internacional desde principios de junio de 2013[2], cuando el ex empleado de la NSA Edward Snowden hizo públicos numerosos documentos que contenían información masiva y privada de los ciudadanos. En estos documentos se detallaba cómo la Agencia recibió alrededor de 250 millones de listas de contactos de ciudadanos[3] al año a través de un programa global de espionaje de las comunicaciones, centrado en la obtención de datos de los ciudadanos mediante la utilización de medios telefónicos y del uso de internet.

---

[1] Directorate General for Internal Policies, *The US surveillance programmes and their impact on EU citizens´fundamental rights*, Policy Department citizen´s rights and constitutional affairs.

[2] Artículo periodístico El País, "Edward Snowden y la UE", 8 julio de 2013.

[3] Artículo periodístico: " La NSA recopiló millones de contactos de cuentas de correo", El Mundo, 6 de febrero de 2014.

Por una parte encontramos la posición de TURNER quien defiende la postura de vigilancia al afirmar que la Agencia: "está centrada en descubrir y desarrollar inteligencia sobre objetivos extranjeros válidos como terroristas, traficantes de personas y traficantes de drogas". "No estamos interesados en la información privada de los estadounidenses"[4]. Por otra parte, desde la perspectiva del TEDH considera que la Agencia ha utilizado métodos ilegales y no racionales para acceder a la información necesaria para la supuesta protección de los ciudadanos[5]. Estos métodos se caracterizan por coaccionar a empresas para robar claves o alterar sistemas informáticos y de este modo acceder a las comunicaciones privadas en la web de ciudadanos de EEUU y de otros terceros Estados[6].

Se hace necesario en este punto mencionar algunas noticias recogidas el día 7 de febrero de 2014[7] en las que se trata de justificar que la NSA sólo recibe el 30% de datos de la información que le es transmitida, en comparación con 2006 cuando recibía toda la información registrada de los ciudadanos norteamericanos. La Agencia justificará su petición al TJUE para que pueda seguir recabando más información.

Junto con la NSA, también se encuentran involucradas en la cuestión del espionaje las agencias británicas *GCHQ* consideradas el puerto de transmisión de información entre Europa y Estados Unidos. Según el informe anual "Enemigos de Internet 2014"[8] esta agencia ha excedido los requisitos recogidos en la ley británica[9] al afirmar que el espionaje producido se considera desproporcionado como se define en el texto:

> *The large-scale wiretapping carried out by GCHQ under the Tempora program[10] clearly contravenes these principles since they are carried on a large scale and systematically, and are thus disproportionate[11].*

---

4 *Op.cit;* D.G for Internal Policies *The US surveillance programmes and their impact on EU citizens´fundamental rights.*

5 Artículo *Privacy Internationa*l. Una guía de privacidad para hispanohablantes. https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/informacion-general-sobre-privacidad.

6 GÓMEZ, J., "EEUU también espió y pirateó comunicaciones de la UE en su sede", El País, 30 de junio de 2013.

7 Artículo periodístico de noticias internacionales, 7 de febrero de 2014 del Wall Street Journal y el Washington Post.

8 Reporteros sin Fronteras, "Enemigos de Internet 2014", publicado el 13 de marzo de 2014.

9 *Regulation of Investigatory Powers Act 2000.*

10 Aclaración de Tempora program: programa que recibe datos de origen de internet.

11 *Op. cit; Enemigos de Internet 2014*, publicado el 13 de marzo de 2014, p. 14.

Como se afirma en dicho informe[12], la NSA viola los requisitos de la *Regulation of Investigatory Powers Act de 2000*. El GCHQ obtiene datos que no ayudan a proteger la seguridad nacional, ni previenen o intervienen posibles peligros terroristas dentro del Reino Unido[13]. La información aportada por el periódico *The Guardian*[14] confirma que los datos corresponden a la vida privada de ciudadanos incluso a detalles secretos de la vida privada del Primer Ministro David Cameron. También el PE[15] advierte en uno de sus informes que las actividades de espionaje británico eran ilegales. La NSA y los GCHQ vulneran el derecho internacional al comprobarse que han espiado a UNICEF o Médicos del Mundo entre otras organizaciones no gubernamentales. También han espiado a embajadas, a la canciller alemana y al primer ministro israelí[16]. Lo revelado demuestra que las agencias utilizan el espionaje con miras más amplias que sólo descubrir terroristas y crímenes potenciales.

El *Washington Post* afirmó en junio de 2013 que la NSA[17] se basa para defender su legalidad en textos jurídicos sobre espionaje como el *Foreign Intelligence Surveillance Act de 1978*, modificado por el *FISA Amendments Act de 2008*, pero existen varias cuestiones en los siguientes informes[18] que proporcionan justificación a la violación del derecho a la privacidad realizada por la NSA junto con otras agencias de espionaje europeas, principalmente la británica *GCHQ*.

La NSA ha utilizado a compañías y agencias privadas para conseguir información y cedérsela secretamente a la agencia. Dentro de EEUU, el ejemplo más claro es el de AT&T[19] (servicio pionero de telecomunicación estadounidense) que vulneró la vida privada de los clientes proporcionando información privada a través de las redes

12 Ibid; *Supra* nota 11, p. 15.

13 Véase el artículo " EEUU y Reino Unido espiaron a Israel, la UE, la ONU y Médicos del Mundo", 20 de diciembre de 2013. Se comprueba cómo vigilan para otras funciones diferentes a la lucha contra el terrorismo.

14 http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance.

15 Ibid; *Supra* nota 12, p. 17.

16 *Op.cit;* EEUU y Reino Unido espiaron a Israel, la UE, la ONU y Médicos del Mundo, 20 de diciembre de 2013.

17 *Op.cit; "* Artículo periodístico de noticias internacionales[…]"

18 *Op. Cit; Enemigos de Internet 2014* publicado el 13 de marzo de 2014 y en *The US surveillance programmes and their impact on EU citizens'fundamental rights.*

19 Véase también el caso de la compañía telefónica *Verizon* que cedía datos personales de las llamadas telefónicas tanto nacionales como internacionales.

telefónicas a la NSA. La NSA ha contactado con agencias europeas[20] como la alemana *Bundesnachrichtendienst,* participando en un 20% del acceso a Internet, con la *Swedish agency FRA*, teniendo acceso privilegiado a los cables submarinos en el Báltico y la compañía francesa *France´s DGSE*, intercambiando información entre Estados. Por tanto, SOLOVE[21] afirma que la vulneración principal de la NSA es la captación de escuchas telefónicas, tanto nacionales como internacionales y el uso de empresas privadas para conseguir información secreta de ciudadanos.

Como aparece en el informe [22], la NSA adultera su objetivo de luchar contra el terrorismo que por su condición de organismo de seguridad nacional le corresponde[23]. Por ello se equipara a EEUU con países autoritarios y no democráticos como Etiopía, Arabia Saudí, Rusia, Bielorrusia, Sudán o Colombia. ejemplo éste último donde una unidad de vigilancia digital ha interceptado miles de mensajes entre periodistas.

Edward Snowden, antiguo empleado de la NSA, destapó la caja de los truenos al cuestionar públicamente el uso del espionaje de EEUU y posteriormente del Reino Unido. Sus revelaciones causaron un debate a nivel mundial sobre el enfrentamiento claro entre el derecho a la privacidad reconocido en las democracias y la defensa estatal de la seguridad en la lucha para evitar el terrorismo. Lucha que se acrecentó como se ha mencionado tras el 11 de septiembre de 2001 que causó la adopción por EEUU de políticas de seguridad más intensas y del uso estatal del avance de las tecnologías y del comercio electrónico.

Snowden es considerado un *whistleblower* definido por UGARTE como: "personas que acceden a la información privilegiada sobre algún tipo de delito o comportamiento inadecuado que se realiza al amparo de los secretos oficiales y de espaldas al público"[24]. El caso de Snowden es similar al precedente de Daniel Ellsberg, que reveló los "Papeles del Pentágono". Éste último, en cambio, acabó entregándose a las autoridades al tener

---

[20] *Op.cit;* " EEUU y Reino Unido espiaron a Israel, la UE, la ONU y Médicos del Mundo", 20 de diciembre de 2013.

[21] SOLOVE J., *Nothing to Hide*, "*The false tradeoff between privacy and security"*. Yale University Press, 2011.

[22] *Op. cit;* Reporteros sin Fronteras, *Enemigos de Internet 2014*.

[23] Véase los casos de espionaje expuestos en: "El goteo de filtraciones que fraguó el escándalo de espionaje", El País, 17 de enero de 2014.

[24] Artículo *Nueva Sociedad*, Nº247, septiembre-octubre de 2013, ISSN: 0251-3552.

certeza de que la información recopilada iba a ser publicada. El caso de Snowden también se diferencia con el de Assange en el tipo de documentos que revelan. Como muestra CERVERA[25] Assange revela principalmente información sobre la guerra de Irak haciendo públicos crímenes de guerra, mientras que los documentos publicados por Snowden hacen referencia a comportamientos abusivos e ilegales del espionaje cometido por la NSA. Como afirma dicho autor:

> la documentación demuestra un extenso y profundo compromiso con la recolección de todo tipo de materiales, dentro y fuera de los Estados Unidos […]Y todo ello sin que haya una justificación medio razonable de la utilidad de semejante y desmedido abuso de la privacidad a escala planetaria [26] .

Por tanto, las principales justificaciones que nos permiten afirmar que los documentos revelados por Snowden implican una vulneración a la privacidad son las expuestas en el informe del Parlamento Europeo[27]:

En primer lugar, las revelaciones de Snowden sobre el programa PRISM[28] muestran que el espionaje a escala trasnacional suponen vulneraciones de derechos fundamentales. Nos centramos exclusivamente en la vulneración de privacidad a ciudadanos europeos por encontrarse en este caso en una situación más frágil de protección que los ciudadanos norteamericanos al destacar: "*any citizen of the EU has the right to have a private life", "a life which is not fully under the surveillance of any state apparatus"* [29]. Por ello, la primera justificación es la utilización de programas de vigilancia como PRISM[30] utilizados para funciones distintas a la lucha contra el terrorismo como se expone en el informe:

> *PRISM seems to have allowed an unprecedented scale and depth in intelligence gathering, which goes beyond counter-terrorism and beyond espionage activities carried out by liberal regimes in the past* [31].

Otra de las justificaciones que suponen la violación del derecho a la privacidad de ciudadanos europeos es el riesgo que supone la utilización del programa *cloud*

---

25 CERVERA J, *Assange contra Snowden: parecidos y diferencias*, El diario, 7 de enero de 2014.

26 Artículo periodístico de noticias internacionales, del Wall Street Journal y el Washington Post, 7 de febereo de 2014.

27 *Op. Cit*; *The US surveillance programmes and their impact on EU citizens´fundamental rights* […]

28 Veáse el significado: programa de vigilancia de internet utilizada por la NSA.

29 *Op.cit; The US surveillance programmes* […] p.8.

30 Veáse otros programas de vigilancia como: *Upstream, Xkeyscore, BULLRUN, Boundless Informant o MUSCULAR* que se han excedido en sus funciones vulnerando el derecho humano a la privacidad.

31 Ibid; *Supra* nota 31 " The US surveillance […] rights" p. 8.

computing[32] que deja a los ciudadanos no americanos sin poder reclamar judicialmente en las cortes americanas. Es necesario destacar el informe del LIBE[33] en 2012 en el que se menciona que dicho programa mencionado junto con las regulaciones americanas presentan una amenaza sin precedentes a la soberanía de datos de la UE al afirmar:

> *(Cloud providers) cannot fulfill any of the privacy principles on which Safe Harbour is founded. The root problem is that cloudcomputing breaks the forty year old model for international data transfers*[34].

Es necesario también mencionar que la Cuarta Enmienda de la Constitución Americana implica la no realización de *unreasonable searches and seizures.* Esta medida no es aplicable a ciudadanos europeos, quienes no reciben por parte de EEUU el derecho a un recurso efectivo. Este derecho es fundamental en el marco jurídico europeo mientras que EEUU recíprocamente niega a los ciudadanos europeos que no residen en su país dicho derecho. Como expone MORAES:

> La reciprocidad es una característica esencial de las relaciones internacionales y algo de lo que ha carecido fundamentalmente la relación entre la UE y los Estados Unidos. Mientras que la protección jurídica de los Estados Unidos con respecto a los datos de las comunicaciones se aplica solo a los ciudadanos estadounidenses y residentes, en la UE se protegen como derechos fundamentales los datos personales y la confidencialidad de las comunicaciones de todo el mundo con independencia de su nacionalidad[35].

Por último, en conexión con lo anterior es de necesidad mencionar a PRASOW[36] en cuyo informe de *Human Rights Watch* confirma las vulneraciones de los documentos revelados por Snowden al exponer:

> *The mass communications surveillance revealed by Edward Snowden demonstrates a shocking disregard by the US for the privacy rights of both those inside the country and those abroad. Documents released by Snowden, the former National Security Agency contractor, have revealed several programs that systematically gather private information on many millions of people worldwide without any particular justification* [37].

---

32 *Op.cit;* Artículo *Nueva Sociedad*. Veáse el significado: "*distributed processing of data on remotely located computers accessed through the Internet"*, p.21.

33 DIDIER B. A.A.V.V *Fighting Cyber crime and protecting privacy in the cloud* Study for the European Parliament, PE 462.509.

34 *Op.cit;* The US surveillance […] rights p. 22

35 MORAES, C., *Sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos,* Documento de Trabajo para el PE, 11 de diciembre de 2013, p. 10.

36 PRASOW, senior national security counsel and advocate at Human Rights Watch.

37 Human Rights Watch; US: "*Surveillance practice violates Rights"*, 12 of March 2014.

Una de las consecuencias del espionaje masivo realizado por la NSA ha producido que el Parlamento Europeo, el 13 de marzo de 2014, amenazara a EEUU con bloquear el importante acuerdo de libre comercio entre EEUU y la UE si la NSA no cesa su vigilancia digital. En este mensaje se destaca la importancia de la protección de la privacidad a los ciudadanos europeos por el presidente del Parlamento CHULZ al decir: "Como europeos, debemos tener más determinación a la hora de promover nuestros valores y de proteger nuestros ciudadanos tanto cuando están *on line* como cuando no"[38].

Consideramos que el espionaje llevado a cabo por la Agencia de seguridad americana vulnera la privacidad de los ciudadanos europeos y que la colaboración entre agencias de espionaje para obtener información privada de consumidores ha excedido sus funciones sin ceñirse a la lucha contra el terrorismo. Una vez comentado uno de los supuestos más problemáticos en relación con la vulneración al derecho de privacidad, nos centramos en analizar dos acuerdos considerados de relevancia en nuestro trabajo al tratar de la transmisión de datos entre EEUU y la Unión Europea realizando previamente una breve introducción a la protección de datos.

1.2 Problema en la transmisión de datos y los Acuerdos suscritos entre la Unión Europea y los Estados Unidos:

Como se expone en el informe[39] durante la época de 1960 y 1970 se incrementa el interés generalizado por el derecho a la privacidad tras el avance de las tecnologías. Dicho desarrollo experimentado principalmente por los Estados occidentales ha llevado a crear la sociedad de la información en la que el crecimiento exponencial de la información y la posibilidad de acceder con mayor facilidad a la misma ha llevado a crear nuevos retos a la protección de datos. La mera existencia de internet y el proceso de la globalización han cambiado el panorama jurídico generando nuevas amenazas a la privacidad de los individuos.

---

38 Artículo periodístico de "El País", miércoles 13 de marzo de 2014.

39 POLONETSKY., *Privacy and the Age of Big Data, A time for big decisions*, Standford Law Review.

Aunque las legislaciones varíen según los Estados, todas exigen que la información personal deba ser obtenida de manera legal, utilizada solo para el específico propósito original, adecuada, relevante y no excesiva para su propósito, exacta, actualizada, accesible al sujeto, mantenida de forma segura y destruida después de que haya logrado su propósito.

Después de analizar la protección de datos, cabe estudiar el problema originado por la transmisión de datos entre los países miembros de la UE y los EEUU, considerado el punto central de los acontecimientos fácticos explicados con anterioridad al principio del capítulo. Para ello, nombramos los dos Acuerdos logrados entre Estados Unidos y la Unión Europea: el Acuerdo de "Puerto Seguro" y el Acuerdo "SWIFT".

1.2.1 Problema en la transmisión de datos y el Acuerdo de Puerto Seguro.

Antes de centrarnos en el Acuerdo de Puerto Seguro, explicamos el problema que surge cuando se transmiten datos a terceros Estados. Las transmisiones de datos electrónicos se realizan con facilidad al superar las fronteras de terceros países que no disponen de leyes de protección donde la información se puede transmitir libremente, pero generan preocupación en aquellos países que sí tienen leyes de protección de datos que puedan ser vulneradas.

Los Estados miembros del Consejo de Europa encuentran protección de su privacidad en el art. 12 de la Convención de 1981 de dicho Consejo donde se establecen ciertas restricciones a la definición de la privacidad de ciudadanos europeos cuando se transmita a países fuera de Europa en el párrafo que contempla:

> Los Estados Miembros deben estipular que la transferencia de datos personales a un tercer país que los esté procesando o tenga la intención de procesarlos después de transferidos, solo debe realizarse si el tercer país en cuestión asegura un nivel adecuado de protección[40].

Lo que se intenta destacar es que el nivel de protección en el país de destino debe ser

[40] Consejo de Europa, Convención para la Protección de Individuos con relación al Procesamiento Automático de Datos Personales 1981.

"adecuado" y no por tanto "equivalente". Si no se consigue ese nivel de protección adecuado, otra de las formas de proteger la privacidad de la información que se transmite a terceros países es mediante un contrato privado con clausulas contractuales de protección de datos.

Cabe destacar el problema surgido con la transmisión de datos de los pasajeros europeos al gobierno de Estados Unidos. Debido a la tragedia del 11 de septiembre, EEUU adopta la *Aviation Transportation Security Act*, siendo reformada por la *Homeland Security Act* de 2002 junto con otras leyes como el *Executive order* de 2005 sobre la cooperación entre organismos de los Estados Unidos en la lucha contra el terrorismo. Esto plantea un enfrentamiento entre las normas protección de datos y estas normas de seguridad cuyo fin es la prevención del terrorismo y otros delitos graves de carácter internacional. Debido a esta situación se inició un Acuerdo entre EEUU y la Unión Europea, aprobado el 14 de mayo de 2004 por la Decisión 2004/535/CE concluyendo que la Oficina de Aduanas y de Protección de Fronteras de EEUU sí que ofrecía un nivel adecuado de protección de los datos transmitidos por ciudadanos europeos. En el Acuerdo se recogía en el primer punto:

> respetar los derechos y libertades fundamentales, en particular la intimidad , al tiempo que se previene y combate el terrorismo y los delitos relacionados con el terrorismo y otros delitos graves de carácter transnacional , incluido el crimen organizado[41].

Dicho Acuerdo fue anulado por la Sentencia del Tribunal de Justicia de la Unión Europea de 30 de mayo de 2006 junto con el apoyo del Parlamento Europeo en contraposición del Consejo y de la Comisión. El TEDH adoptó un único argumento para anularlo pues el Acuerdo tenía una "*inadecuada base jurídica*" ya que los fines de seguridad pública y tutela penal se encuentran excluidos de la aplicación de la Directiva 95/46/CE. Tampoco era suficiente basarse en el artículo 95 del Tratado constitutivo de la Comunidad Europea como base legal para el Acuerdo.

Desde el 1 de octubre de 2006 hasta el 1 de enero de 2008 no existió Acuerdo alguno hasta la aprobación de la Decisión 2007/551/PESC/JAI del Consejo de 23 de julio al fundamentar un nivel de protección adecuado de los datos transferidos basado en las

[41] Decisión 2004/496/CE del Consejo, de 14 de mayo de 2004.

garantías de la carta del Departamento de Seguridad del Territorio Nacional Estadounidense.

De este Acuerdo de protección de los datos transmitidos surgen dudas y críticas como se expone en el informe,[42] debido a que EEUU no tiene una normativa sobre protección de datos de carácter personal de aplicación en todo el territorio y en todos los sectores de actividad, sino normas dispersas aplicables a sectores concretos. En segundo lugar en EEUU no existe agencia supervisora alguna de la privacidad de la información personal, sino que rige el sistema de protección sectorial. Por último, concluimos la existencia de una disminución de las garantías del derecho fundamental sustentándose en el Dictamen 5/2007 de 17 de agosto, al haber aumentado el número de datos transferibles, incluyendo datos considerados personales y sensibles, cuya filtración puede ser utilizada por las autoridades norteamericanas.

Aunque con este Acuerdo no se dota de protección y garantía suficiente, se intenta buscar el equilibrio entre privacidad y seguridad. Se han dado lentos avances y afirmamos junto con el Grupo de Trabajo sobre Protección de Datos[43] que las garantías protegidas plantean dudas ya que como afirma dicho Grupo: "despertará recelos comprensibles en todos los viajeros transatlánticos preocupados por su derecho a la privacidad"[44].

1.2.2 Acuerdo "SWIFT" (*Society for Worldwide Interbank Financial Telecommunications*) entre la Unión Europea y los Estados Unidos para la transmisión de información financiera.

Una vez analizado el acuerdo de transmisión de datos de carácter personal, nos centramos en estudiar el acuerdo de transmisión de datos relativo a la información financiera.

---

42 *Op.cit;* Directorate General for Internal Policies, *The US surveillance programmes and their impact on EU citizens´fundamental rigths*, p. 25-27.

43 Grupo de trabajo del Artículo 29: órgano consultivo compuesto por un representante de las autoridades de control de los Estados Miembros, el Supervisor Europeo de Protección de Datos y la Comisión.

44 BALLESTEROS; "*Hacía un difícil equilibrio entre privacidad y seguridad*": la conservación de datos en las comunicaciones electrónicas y la transferencia de datos de pasajeros por las compañías aéreas, p. 55

El llamado Acuerdo "SWIFT", en vigor desde el 1 de agosto de 2010, firmado por el Consejo de Europa, tras recibir la aprobación por el Parlamento Europeo junto con los Estados Unidos, recoge los requisitos esenciales sobre la transmisión de datos financieros desde la sede del consorcio bancario SWIFT, actualmente en Bélgica, a los EEUU. Previo al Acuerdo de 2010, existía el Acuerdo SWIFT de 2009, sustituido por el presente, al mejorar las condiciones en materia de protección de datos, obtener la ratificación del PE y la posibilidad de que éste pudiera participar activamente en las negociaciones.

El problema que suscita la necesidad de dicho Acuerdo surge tras la adopción por EEUU de una política más segura y seria, fruto del ataque terrorista del 11 de septiembre, para combatir el terrorismo y su financiación.

Es necesario en este apartado mencionar a PÉREZ DE NANCLARES al determinar que el objeto de dicho Acuerdo es:

> establecer un marco jurídico que permita la entrega a los Estados Unidos de los datos de mensajería financiera sobre transferencias financieras almacenados en el territorio de la Unión Europea [...][45].

Los EEUU se obligan a poner a disposición de las autoridades europeas responsables de la lucha contra el terrorismo de los Estados Miembros, del EUROPOL o del EUROJUST de la información que se obtiene a través del programa TFTP[46].

Junio de 2006 es la fecha en la que comienza el conflicto principal con dicho Acuerdo. Como destaca VARA,[47] la prensa reveló la existencia del TFTP y el acceso secreto por parte de la Administración estadounidense a los datos almacenados por SWIFT. Esto supuso la masiva violación de la legislación europea de protección de datos y la vulneración de la Directiva 95/46 del PE y del Consejo de Europa en una Resolución del PE adoptada en 2007 expone que: "las empresas que operan a ambos lados del Atlántico se ven confrontadas cada vez con mayor frecuencia a requisitos jurídicos

---

45 PÉREZ DE NANCLARES., *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, p. 355-375.

46 Véase el significado de TFTP: *Terrorist Finance Tracking Program*.

47 VARA., *La transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos*, Cátedra Telefónica de la Universidad de Salamanca, p.9.

contradictorios de las jurisdicciones de los EE.UU y la CE"[48].

Debido a la vulneración producida en materia de protección de datos y la incertidumbre legal existente, la Comisión Europea llega a un Acuerdo con EEUU con el objetivo primordial de proporcionar garantías en materia de protección de datos.

Por lo expuesto, EEUU comienza a tomar medidas para evitar dichas vulneraciones[49]. En primer lugar, EEUU comprueba que el programa TFTP es un instrumento eficaz para luchar contra la financiación del terrorismo y que la solicitud de datos bancarios de clientes europeos debe estar motivada y utilizada únicamente para la lucha contra futuros ataques terroristas. En segundo lugar, la solicitud tiene que ser remitida al EUROPOL para que apruebe si las solicitudes por el gobierno estadounidense cumplen con lo establecido en el Acuerdo. Por último, EEUU acepta que se nombre a una "personalidad eminente europea" con el objetivo de verificar que la utilización del TFTP no vulnera la legislación europea en materia de protección de datos.

Consideramos que no es fácil alcanzar un acuerdo satisfactorio entre la lucha contra el terrorismo y su financiación y la protección de datos personales. Sin embargo, el contenido de dicho Acuerdo SWIFT sigue dando prioridad a la seguridad sobre la respectiva protección de los derechos fundamentales.

Aún así, el desarrollo de estos dos Acuerdos en materia de transmisión de datos supone un importante avance en la cooperación entre EEUU y la Unión Europea incentivando las relaciones internacionales entre ambos, tratando de marcar el límite de hasta dónde un Estado es legítimo para recibir datos personales de los ciudadanos y evitando las intromisiones y filtraciones masivas.

A continuación, exponemos uno de los desarrollos a nivel tecnológico más importantes en relación con los cuatro supuestos técnicos expuestos: el comercio electrónico.

---

[48] Ibid; *Supra nota* 40 p. 9.

[49] *Op.cit;* VARA J.S, La transferencia de datos […] p.10-11.

1.3 Los peligros de Internet en la intromisión de la vida privada de las personas: el desarrollo del comercio electrónico.

En relación con los casos mencionados de la NSA, Snowden y los Acuerdos de transmisión de datos, el Estado norteamericano y, posteriormente el británico, reciben información secreta a través de Internet y el llamado comercio electrónico.

RODRIGUEZ, expone:

> vivimos en la sociedad del riesgo. Nuevas amenazas como el terrorismo, el cybercrimen o los desastres medioambientales han venido a unirse a riesgos más tradicionales como las enfermedades o la delincuencia[50].

Frente a la nueva amenaza el terrorismo internacional, la seguridad se ha convertido en uno de los grandes valores que son protegidos través de los avances tecnológicos. Nos encontramos cada vez más ante una tecnología denominada por dicho autor[51] "invasiva" que pone en riesgo el derecho a la privacidad de los ciudadanos, así como la protección de datos. Se trata de alcanzar un equilibrio entre privacidad y seguridad para evitar que los Estados se involucren en asuntos delicados y privados que no tengan como objetivo limitar el terrorismo como riesgo creciente en la sociedad en la que vivimos.

La utilización de Internet debe hacerse con precaución porque aunque permite a los ciudadanos manejar cantidad de información y realizar transacciones transfronterizas puede llevar a entrometerse en la vida privada de las personas. Como define MURILLO DE LA CUEVA:

> ante la falta de niveles de seguridad adecuados, cualquiera que llegue a disponer de esos datos pueda volverse un terrorista o un gamberro y producir notables perjuicios públicos y privados. El Peligro no es ya el *Big Brother* orwelliano, sino los muchos *little brothers* que pueden acabar surgiendo[52].

Vivimos en una sociedad que como define URRIBARI es:

> la sociedad de la Información, ya que el uso de la internet resulta imprescindible para realizar numerosas actividades profesionales y personales que afectan directamente a nuestro modo de vida[53].

---

50 RODRÍGUEZ, M.A., "Intimidad, protección de datos y seguridad: un difícil equilibrio", p.1384-1387.

51 *Op.cit;* VARA; La transferencia de datos de mensajería financiera […] p. 18.

52 FRIEDMAN T.L, *Hacker Lesson: Wired citizens Needs Government*, 16 of February 2000.

53 *Jornadas sobre protección de la privacidad*, capítulo "La protección de datos en Internet y en los demás servicios de Telecomunicaciones", Agencia de Protección de datos, 2000, p. 40- 42.

Queremos destacar que el comercio electrónico a menudo supone una vulneración a la privacidad como derecho humano. En lo relativo a internet, entendido ésta como un servicio público y como el principal instrumento de comunicación y de acceso a la información y a la libertad de expresión, LA RUE, relator especial de la ONU, planteó en su informe[54] el avance de la tecnología que permite a los estados monitorear comunicaciones privadas siendo la seguridad nacional una obligación del Estado al proteger a los individuos por una parte y al sistema democrático por otra. LA RUE plantea que el comercio electrónico supone una amenaza por parte de los Estados al vigilar las comunicaciones de las personas. Como el comercio electrónico y los medios de comunicación continúan creciendo, la ONU cree que se tiene que alcanzar un equilibrio entre la protección a la privacidad y la garantía de la seguridad ciudadana. LA RUE discute en dicho informe[55] que sin legislación adecuada para garantizar la privacidad y la libertad de expresión, periodistas, defensores y denunciantes de los derechos humanos no pueden tener la seguridad de que sus comunicaciones no estarán sujetas a la investigación del Estado. Además, no sólo se requiere una legislación adecuada sino que también se les notifique a los individuos cuándo se interfiere en sus comunicaciones privadas y en situaciones excepcionales, se requerirá la supervisión judicial. Por último, se requiere una mayor protección en la era digital del comercio electrónico y de internet compartiendo la postura de FLYNN-SCHNEIDER en cuyo artículo expone:

> In today's online world, digital privacy rights may need to be more comprehensively protected in order to meet international human rights standards guaranteed to individual privacy and freedom of speech[56].

Con este apartado queremos dejar claro que aunque los estados y autoridades gubernamentales utilizan internet y el llamado *commercial e-commerce* con el objetivo de garantizar la seguridad nacional, la privacidad es una barrera necesaria ante el control y la dominación del Estado para evitar las sucesivas vulneraciones al derecho de privacidad que hemos mencionado previamente. Más adelante en el trabajo,

---

54 LA RUE F., Informe ante el Consejo de Derechos Humanos de Naciones Unidas: *Incidencia de la Vigilancia Estatal de las Comunicaciones en el Derecho a la Privacidad y el Derecho a la Libertad de Expresió*n, 2012.

55 *Op.cit;* VARA, La transferencia de datos de mensajería financiera […], p.22.

56 SCHNEIDER F., *Intergovernmental organizations*, American University Washington College of Law, Human Rights Brief, p.2.

expondremos algunas soluciones propuestas con el objetivo de minorar las vulneraciones a la privacidad cometidas por la era digital y las nuevas tecnologías.

Una vez analizado el capítulo preliminar donde hemos querido explicar las cuestiones técnicas- jurídicas, pasamos a realizar el estudio de la fundamentación jurídica donde analizamos en el capítulo primero la protección al derecho de privacidad y en el capítulo segundo procederemos a examinar las limitaciones para una posible intervención en la esfera privada de las personas.

CAPÍTULO PRIMERO: FUNDAMENTACIÓN JURÍDICA DEL DERECHO A LA PRIVACIDAD.

Se analizará el concepto de privacidad y posteriormente la protección jurídica tanto a nivel internacional, regional y europeo que recibe dicho derecho, recalcando las vulneraciones cometidas.

1. Concepto de privacidad: tipos y modelos de protección en general.

El derecho a la privacidad es considerado un derecho humano relacionado con otros derechos como la libertad, tanto de expresión como de asociación. Es un derecho reconocido en prácticamente todos los textos constitucionales de todos los países y en aquellos Estados que no lo regulan ha sido necesaria la labor de la jurisprudencia para protegerlo en otros textos legales.

Las definiciones de privacidad son amplias pero podemos definirla como un derecho que conlleva una protección esencial de la esfera privada del individuo frente a posibles intromisiones de los poderes públicos. BRANDEIS define privacidad como: "el derecho a ser dejado solo o ser dejado en paz" y sostiene que "era una de las libertades más apreciadas en una democracia" y "una parte integral de nuestra humanidad, el corazón de nuestra libertad y el comienzo de toda libertad"[57].

[57] AGUSTINA, J.R., (Dir) *Tendencias en prevención del delito y sus límites, Privacidad y dignidad humana frente al uso de las nuevas tecnologías*, agosto 2010.

Existen diversos tipos de privacidad[58] y destacamos en el tema que nos concierna la privacidad de la información y de las comunicaciones. La primera consiste en el establecimiento de límites al recoger información y manejar datos personales como registros gubernamentales o de la sociedad, conocida también como "protección de datos". En cambio, la segunda hace referencia a la seguridad y privacidad del correo electrónico, llamadas telefónicas u otras formas de comunicación entre las personas. Tanto la privacidad de información como de comunicación han sido vulneradas por la NSA y las agencias de seguridad europeas como se ha expuesto en el capítulo preliminar al recabar información de forma secreta e indiscriminada manejando dichos datos para fines distintos a la lucha contra el terrorismo.

Citamos la postura doctrinal de PRATS quien sostiene la evolución del concepto de privacidad como derecho en dos vertientes. Por un lado, la privacidad se enmarca en la esfera de libertad negativa y el concepto de *privacy* se entiende como: "*to be let alone*, dotada de un contenido de exclusión, como garantía y defensa de la esfera de la vida privada y de las injerencias externas"[59]. Por otro lado, encontramos el concepto de privacidad en la esfera de libertad positiva al concebir la privacidad como:

> una libertad positiva para ejercer un derecho de control sobre la información y los datos referidos a la propia persona, incluso los ya conocidos, esto es, que han salido ya de la esfera de la intimidad, para que sólo puedan utilizarse conforme a la voluntad de su titular[60].

A continuación se analizarán sentencias del TEDH que intentan dotar a la privacidad de una mayor protección y regulación.

En el ámbito general la privacidad queda protegida por diferentes modelos de protección y, dependiendo de los Estados se utilizarán unos u otros. La mayoría de los Estados Miembros de la Unión Europea utilizan el modelo de protección de leyes integrales, en los que una ley general regula toda la información que recibe del sector público y privado, teniendo cada Estado una entidad que supervisa su cumplimiento. Otro de los modelos de protección es el de leyes sectoriales utilizado por EEUU y que se caracteriza por la no existencia de reglas generales de protección de la privacidad y la

---

[58] Artículo Privacy International. Una guía de privacidad para hispanohablantes. https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/informacion-general-sobre-privacidad.

[59] PRATS, F., *La tutela penal de la intimidad: privacidad e informáti*ca, ed. Destino, Barcelona, 1984, págs. 15 y ss.

[60] *Op.cit*; PRATS, *La tutela penal (...), p. 16-18.*

carencia de una agencia supervisora para fortalecer la privacidad. En este modelo de protección para cada cuestión relacionada con la privacidad se aplica una nueva ley que la va a regular. Por ejemplo, en EEUU no hay una regulación estatal sobre esta materia, las compañías se autorregulan mediante códigos de conducta[61]. Junto con estas leyes sectoriales, cabe destacar cómo el término privacidad en sí no queda regulado en la Cuarta Enmienda de la Constitución Americana sino que protege los registros llevados a cabo por el Estado siempre que la persona mantenga "una expectativa razonable de privacidad"[62] siendo según la sentencia Katz contra United States: "expectativa real de privacidad" y "esa expectativa debe ser tal que la sociedad esté predispuesta a reconocerla como razonable"[63].

De estos dos modelos de protección consideramos junto con el autor del informe[64] mencionado que existen tres razones fundamentales por lo que los países deben optar por aplicar el modelo de ley integral y no el de ley sectorial. La primera razón sería para reparar antiguas injusticias. Muchos países, especialmente en Europa Central, América Latina y el Sur de África están adoptando dicho modelo de protección para reparar violaciones a la privacidad que surgen por vivir inmersos en regímenes autoritarios y carecen de una agencia que se encargue de supervisar dicha protección. La segunda razón para incrementar la protección del comercio electrónico debido a la preocupación de los Estados al reconocer que los consumidores están preocupados con el aumento de la disponibilidad de sus datos personales, especialmente con los nuevos medios de identificación y formas de transacción. La ultima razón es para garantizar leyes que sean consistentes con las leyes de ámbito regional, adoptando nuevas leyes basadas en el Convenio del Consejo de Europa y la Directiva de Protección de Datos de la Unión Europea, considerados esenciales en la protección internacional del derecho a la privacidad.

---

61 JIMÉNEZ, C., "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información", Universidad de Huelva, p.47.

62 Cuarta Enmienda a la Constitución Americana de 1791.

63 Sentencia Katz v. United States 347 (1967)

64 AGUSTINA, J.R., *Tendencias en prevención del delito y sus límites, Privacidad y dignidad humana frente al uso de las nuevas tecnologías*, y *opt.cit;* "Artículo Privacy International […]".

Una vez analizado el concepto de privacidad, los tipos y los modelos de protección a nivel general, estudiamos la protección jurídica destacando los principales textos jurídicos que la regulan y la dotan de protección.

2. Protección jurídica del Derecho a la Privacidad.

A continuación nos centramos en analizar la protección jurídica del derecho a la privacidad para concluir si el espionaje cometido por la NSA junto con las agencias europeas, las revelaciones de Edward Snowden y los Acuerdos mencionados han vulnerado dicho derecho. Comenzamos explicando la protección en el marco internacional y posteriormente, estudiamos a través de jurisprudencia y doctrina la protección en el ámbito europeo.

2.1 Protección a nivel internacional.

A nivel internacional la privacidad encuentra su reconocimiento en la DUDH de 1948, protegiendo la privacidad territorial y de las comunicaciones en su art. 12 al citar:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques[65].

Destacamos otros tratados internacionales que también protegen dicho derecho. En primer lugar, el Pacto Internacional de los Derechos Civiles y Políticos, cuyo art.17 otorga un concepto de privacidad en términos idénticos al CEDH. En segundo lugar, encontramos tratados más específicos que se encargan de dotar de protección a unas personas determinadas como la Convención Internacional de Naciones Unidas sobre la Protección de todos los Trabajadores Migratorios y sus Familias destacando en su art. 14 que: "Ningún trabajador migratorio o familiar suyo será sometido a injerencias

[65] DUDH, adoptada y proclamada por la Resolución 217 A (III) de la Asamblea General el 10 de diciembre de 1948.

arbitrarias o ilegales en su vida privada […] Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques." [66]

También es de importancia mencionar la Convención de las Naciones Unidas para los Derechos del Niño dónde en su art.16 garantiza el derecho a la privacidad de los niños concretamente al decir: "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada [...] El niño tiene derecho a la protección de la ley contra esas injerencias o ataques"[67].

Observamos que los legisladores de los tratados internacionales mencionados han dotado al derecho de la privacidad de una protección global.

Antes de centrarnos en la protección europea, cabe mencionar la iniciativa de privacidad del Foro de Cooperación Económica Asia-Pacífico (*en inglés, APEC*)[68] integrado por 21 economías que en el año 2004 estableció un Marco en materia de privacidad del Asia-Pacífico basándose en las Directrices de la Organización para la Cooperación y el Desarrollo Económico (*en adelante, OCDE*) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980. Como destaca SOLOVE[69] esta iniciativa de privacidad de la APEC tiene potencial para el desarrollo de sólidas leyes que protejan la privacidad en aquellas economías de la APEC que proporcionaban poca protección a dicho derecho. Este marco nos ayuda a encontrar soluciones al debate entre la protección a la privacidad y los beneficios económicos del comercio que involucran datos de información personal con mayor facilidad.

Debemos hacer referencia al derecho interno de los Estados Unidos al ser principal en las cuestiones fácticas explicadas en nuestro capítulo introductorio. Diversas leyes otorgan protección a la privacidad siendo las más reconocidas la *Privacy Protection Act y la Right to Financial Privacy Act*, ambas de 1978 como el *Electronic Communications Privacy Act of 1986*. Por último, la Convención Americana sobre Derechos Humanos

---

66 Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familias, aprobada por la Asamblea General por Resolución 45/158 del 18 de diciembre de 1990.

67 Convención de los Derechos del Niño, adoptada y abierta a la firma, ratificación e incorporación por la Asamblea General por Resolución 44/25 del 20 de noviembre de 1989, entrada en vigor 2 de septiembre de 1990.

68 Asia-Pacific Economic Cooperation de 1989.

69 SOLOVE J., capítulo: " Privacidad, un concepto difuso". *Tendencias en prevención del delito y sus límites.*

estipula una protección al derecho a la privacidad muy similar a la de la DEDH en su art.11.

2.2 Protección a nivel europeo:

El estudio se centra en este apartado en la protección a la privacidad en el marco normativo europeo dado que las vulneraciones producidas por la NSA y las agencias europeas afectan a ciudadanos europeos, al no recibir éstos protección por EEUU. Además, aunque los Acuerdos suscritos entre EEEUU y la UE han supuesto ciertas mejorías en la transmisión de datos, continúa habiendo vulneración por parte de EEUU de la privacidad de personas europeas. Analizamos primero el marco jurídico del Consejo de Europa para adentrarnos seguidamente en el ámbito de la UE.

2.2.1 Consejo de Europa: Tribunal Europeo de Derechos Humanos y Convenio Europeo de Derechos Humanos.

Analizaremos la protección que recibe el derecho a la privacidad en el ámbito exclusivamente europeo para otorgar protección a los ciudadanos que han sufrido vulneraciones dentro de este marco legal mencionando sentencias resueltas por el TEDH.

En primer lugar, el derecho a la privacidad se regula en el art. 8 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales (*en adelante*, CEDH) de 1950 donde se define como:

> 1.Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2.No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino 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 de las infracciones

penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás[70].

La definición propuesta en este artículo nos sirve de base para analizar dos cuestiones principales: en el apartado primero, se garantiza la protección a la privacidad y en el apartado segundo, nos encontramos con las limitaciones a este derecho al garantizar la seguridad nacional y la seguridad pública, necesarias para cualquier sociedad democrática.

Dicho Convenio creó la Comisión Europea de Derechos Humanos y el TEDH para supervisar su cumplimiento a través de la jurisprudencia de dicho tribunal y de posturas doctrinales.

Comenzamos analizando el concepto de "toda persona" y seguidamente el de "derecho al respeto de su vida privada". Por una parte, el carácter de universalidad de los derechos humanos, como el derecho a la privacidad, hace referencia a los titulares de esos derechos, es decir, al carácter universal de "toda persona". Universalidad es una característica para indicar que los derechos humanos se dirigen a una clase de sujetos que deben determinarse materialmente. Esta clase está compuesta únicamente por seres humanos como lo define MEYERS:

> La pertenencia a la especie humana es condición necesaria y suficiente para gozar de los derechos en cuestión, en tanto que otras propiedades -raza, sexo, inteligencia, actos cometidos o padecidos, etc.- son irrelevantes[71].

Por ello, toda persona tiene garantizado el respeto de este derecho universal al poseer un título igual a la posesión de los derechos humanos y también supone afirmar que toda persona goza de dicha protección con independencia de si el beneficiario se encuentra dentro de un sistema jurídico positivo o como define LAPORTA de "condicionamientos institucionales"[72]. Por ello, los ciudadanos europeos que han visto vulnerada su privacidad en los casos de espionaje mencionados previamente en el trabajo sí que encuentran su vida privada protegida por dicho Convenio. Veremos más adelante, cómo no sólo las personas físicas sino también las personas jurídicas gozan de dicha protección.

---

70 CEDH 1950, art.8.

71 MEYERS D., *Los derechos inalienables*. Columbia University Press, 1985. Trad. E. Beltrán, p. 13.

72 *Op.cit*; LAPORTA F., "*Sobre el concepto de los derechos humanos*", p. 32-33.

Pasamos a analizar la segunda parte de la definición: "el derecho al respeto de su vida privada". En el caso Alkaya contra Turquía, de 9 de octubre de 2012, resuelto por el TEDH, existe violación de la vida privada de la demandante al publicarse en los periódicos turcos información sobre su vida privada tal como la dirección de su domicilio y otros datos de su esfera personal. El TEDH concluye en dicha sentencia que el estado de Turquía: "no garantizó a la demandante una protección suficiente y efectiva de su vida privada" [73] . Por tanto, vemos como el estado de Turquía no ha dotado de una protección adecuada para garantizar la privacidad de la demandante. Cabe ponerlo en conexión con las agencias de espionaje europeas mencionadas en el trabajo que no dotaban de protección suficiente cuando transmitían los datos de carácter personal de ciudadanos europeos a la NSA.

Sin duda alguna, el TEDH recuerda haber juzgado en numerosas ocasiones[74] que el concepto de vida privada es: "un concepto amplio, no susceptible de una definición exhaustiva, que engloba en concreto el derecho a la autonomía y al desarrollo personal". También, la Corte Europea ha dado una interpretación extensiva del respeto a la vida privada al mencionar en el caso Niemietz contra Alemania:

> el respeto de la vida privada debe englobar el derecho para el individuo de trabajar y desarrollar relaciones con sus semejantes. No hay ninguna razón de principio de excluir de la vida privada las actividades comerciales o profesionales[75].

Desde una perspectiva doctrinal, cabe destacar la perspectiva de LA RUE, sobre el respeto a la vida privada de las personas al definir:

> in order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files [76] .

LA RUE define más ampliamente el derecho a la privacidad de los ciudadanos destacando dos puntos relevantes: la forma por la cual los ciudadanos deben alcanzar un mayor nivel de protección y la certeza de que su vida privada quede protegida llegando a conocer qué autoridad pública o privada controla sus vidas. Además, en el

[73] STEDH, Alkaya contra Turquia, 9 de octubre 2012, ap. 32.

[74] Véase entre otros, el caso del TEDH, Pretty contra Reino Unido, núm. 2346/02, ap. 61.

[75] STEDH, Niemietz contra Allemagne, 16 de diciembre 1991, ap.30.

[76] LA RUE, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, , United Nations General Assembly, 16 May 2011, p.58.

apartado 57[77] de dicho informe hace referencia a la necesidad de otorgar igual protección a la información recopilada por medio de internet debido a las vulneraciones masivas que se están produciendo a través de estos nuevos medios tecnológicos como el comercio electrónico o el espionaje mencionado previamente en el trabajo.

Una vez hemos analizado los dos elementos principales del derecho a la privacidad, destacamos las vulneraciones del art. 8 del CEDH que el TEDH ha reconocido en determinadas sentencias.

Las transgresiones a la privacidad son producidas por injerencias de las autoridades estatales que, aunque se hayan producido en conformidad con el Derecho interno, violan el derecho a la privacidad protegido en el CEDH. El TEDH concluirá cuándo una injerencia se entiende como lícita y cuándo quebranta los límites recogidos en el apartado segundo del art. 8. Exponemos una de las sentencias resueltas por el TEDH que supone una vulneración al respeto de la vida privada de las personas, por colgar información del demandante en Internet, es el caso K.U contra Finlandia[78]. En la sentencia se menciona que internet es una poderosa herramienta que posibilita la difamación e insulto o la violación del derecho a la privacidad. Por consiguiente, el demandante se quejó conforme al art. 8 del Convenio que se había ocasionado una invasión a su esfera privada sin existir ningún medio efectivo de protección.

Otra de las cuestiones principales es lo que se menciona en el caso Kopp contra Suiza al producirse la ilegalidad de investigaciones y escuchas telefónicas del abogado Kopp. El TEDH indica que el objeto del art.8 es: "proteger al individuo contra la injerencia arbitraria por las autoridades públicas"[79]. Como se expone también en el apartado 72 de la sentencia, las escuchas y las intercepciones en las conversaciones telefónicas suponen una ofensa grave a la esfera de la privacidad como sucedió en las vulneraciones cometidas por la NSA y las agencias europeas al espiar a ciudadanos europeos.

Debemos hacer referencia a las dos teorías sobre la privacidad y ponerlo en relación con la jurisprudencia. Previamente en el trabajo, PRATS se inclinaba por entender la

---

[77] *Op.cit*; LAPORTA F., "*Sobre el concepto de los derechos humanos*", p. 35-37.
[78] STEDH, K.U. contra Finlandia, de 2 diciembre 2008.
[79] STEDH, Kopp contra Suiza, de 25 marzo 1998, ap.64 y ss.

privacidad como libertad positiva y en la sentencia Airey contra Irlanda, de 9 de octubre de 1979, no obliga al Estado a abstenerse de la injerencia arbitraria de la privacidad, es decir, en este sentido la privacidad no adopta la postura de libertad negativa sino que puede haber obligaciones positivas inherentes con respecto a la vida privada o familiar[80]. Por tanto como se recoge en otras sentencias[81] los Estados miembros tienen la obligación positiva de proteger a sus ciudadanos de la vigilancia, realizada por los Estados o por entidades privadas.

Por último, es de mención el caso Valenzuela Contreras, de 30 de julio de 1998, por considerar que:

> la interceptación de la línea telefónica de la empresa en la que trabajaba acordada por virtud de resolución judicial de fecha 19.11.1985 por un Juez de Instrucción de Madrid para investigar un supuesto delito de amenazas e injurias telefónicas y escritas constituía una injerencia del derecho al respeto de su vida privada y de su correspondencia"[82].

En este apartado, hemos podido comprobar la postura jurisprudencial a través de las sentencias resueltas por el TEDH acerca de la primera parte del art. 8 del CEDH sobre el respeto a la vida privada y las vulneraciones producidas. Al ser el espionaje un nuevo medio tecnológico, no hay sentencias del TEDH que resuelva dicha cuestión pero sí hemos podido poner de relieve que existen vulneraciones de la privacidad producidas por la NSA, y las agencias europeas al recabar información por los programas de espionaje. En estos nuevos casos se producen intromisiones injustificadas e ilegítimas de las autoridades públicas en la privacidad de los ciudadanos europeos, marco protegido por el CEDH, vulnerándose los derechos humanos y el Estado de Derecho.

A continuación, nos vamos a centrar en estudiar el marco jurídico a nivel de la UE destacando la privacidad como derecho fundamental y destacaremos el ámbito jurídico sobre protección de datos.

---

[80] STEDH, Airey contra Irlanda, de 9 de octubre de 1979, ap. 32. Véase también la STEDH Marckx contra Bélgica, 13 de junio de 1979, ap.31.

[81] STEDH, Van Hannover contra Alemania, de 24 de junio de 2004; STEDH, X & Y contra los Países Bajos, de 26 de marzo de 1985, 8.

[82] STEDH. Valenzuela Contreras, 30 de julio 1998.

2.2.2 Unión Europea: protección como derecho fundamental y el Derecho Derivado sobre protección de datos.

a) ***Protección como derecho fundamental: Carta de Derechos Fundamentales de la Unión Europea.***

En el ámbito de la Unión Europea cabe resaltar como texto jurídico la Carta de los Derechos Fundamentales de la Unión Europea (*en adelante, CDFUE)*. La principal función de la Carta es codificar los derechos políticos, económicos, civiles y sociales de los ciudadanos europeos y de todas aquellas personas que vivan en el territorio de la Unión. Dentro de estos derechos nos encontramos con el derecho a la privacidad. Dado el gran avance de los medios de comunicación y la insuficiente regulación existente acerca de estos nuevos medios de información, aparecen determinados riesgos y cambios en el contenido clásico de este derecho.

El derecho a la privacidad queda regulado en el art. 7 de la CDFUE como un derecho fundamental al definirlo como: " toda persona tiene respeto a su vida privada y familiar, de su domicilio y de sus comunicaciones"[83]. Este artículo proporciona prácticamente la misma definición que la que da el CEDH, salvo la diferencia de redacción de carácter técnico y la sustitución del término correspondencia por el de las comunicaciones, siendo éste último un concepto más adaptado a los tiempos actuales. Dicho artículo contiene cuatro garantías diferentes, como se expone en el comentario sobre la Carta de Derechos Fundamentales[84]: derecho al respeto de la vida privada, a la vida familiar, al domicilio y al secreto de las comunicaciones. Nos centramos en el apartado del respeto a la vida privada y al derecho de las comunicaciones ya que son los dos temas relacionados concretamente con nuestro capítulo preliminar ya que las vulneraciones explicadas anteriormente atentan contra la privacidad quebrantando el secreto de las comunicaciones mediante los programas de espionaje.

---

83 CDFUE, art. 7.

84 MANGAS M., ALONSO L.N, Carta de los Derechos Fundamentales de la Unión Europea, comentario artículo por artículo, p. 213.

Es necesario hacer referencia a las pocas sentencias que ha resuelto el TJUE en materia de derecho a la privacidad como derecho fundamental, al haber una remisión general de la CDFUE al CEDH que toma como partida el art. 52.3 de dicha Carta al decir:

> en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que le confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa. [85]

Habida cuenta la falta de jurisprudencia por el TJUE, destacamos las sentencias claves de dicha Corte donde encontramos la sentencia Carolina contra Alemania, de 24 de junio de 2004, en la que se garantiza el respeto a todo individuo:

> de un espacio en el que pueda desarrollar su personalidad sin intromisiones externas, que no sólo abarca el recinto estrictamente privado, sino que en cierto sentido proyecta también la protección al espacio público siempre que no conlleve una relevancia social propia o un interés general[86].

Junto con la sentencia mencionada y el caso IPI, de 7 de noviembre de 2013[87], se pretende otorgar una protección al individuo frente a intromisiones ilegítimas de los poderes públicos a través de grabaciones, mecanismos de escuchas u otros medios técnicos. La consecuencia directa es la de proteger a toda persona europea de las intromisiones de los poderes públicos en su esfera íntima y privada. Como sucede en los casos más recientes explicados en la introducción, escuchas telefónicas, vulneraciones cometidas en internet y el desarrollo del comercio electrónico. Esto ratifica la importancia del comentario de la CDFUE que afirma que se podrán adoptar: " medidas positivas suficientes para […] garantizar que no faciliten intromisiones en la vida privada y familiar de terceros"[88].

Estas últimas sentencias podemos ponerlas en conexión con otras pero en este caso ya del TEDH al tratar la protección de las comunicaciones individuales y privadas con terceros que se recogen en la sentencia Klass contra Alemania, de 6 de septiembre de 1978[89] y en el caso de Taylor Sabori, de 22 de octubre de 2002, en las que incluyen

---

85 Artículo 52.3 CDFUE de 2007.

86 STJUE, Carolina contra Alemania, 24 de junio de 2004, ap 57.

87 STJUE, IPI, 7 de noviembre de 2013, C-473/12: vulneración de los detectives por investigar información secreta sin el consentimiento de IPI. Violación de la Directiva 95/46/12.

88 *Op.cit;* MANGAS MARTIN Y GONZÁLEZ ALONSO, Comentario a la Carta […] p. 212.

89 STEDH, Klass contra Alemania, 6 de septiembre de 1978, ap. 27.

comunicaciones más avanzadas como el caso de las conversaciones telefónicas y el correo electrónico no siendo exclusivamente la *correspondencia postal.*

A continuación, expondremos el tema relativo a la normativa jurídica de protección de datos.

b) Derecho Derivado sobre protección de datos.

La segunda cuestión a analizar en este apartado es el Derecho derivado sobre la protección de datos al haberse producido una vulneración constante de ésta por el espionaje informativo realizado por las agencias estatales de seguridad mencionadas. En primer lugar es importante mencionar los dos instrumentos internacionales de protección de datos: la Convención para la protección de las personas con respecto al Tratamiento Automatizado de datos de carácter personal del Consejo de Europa, de 28 de enero de 1981, y las directrices de la OCDE.

Por consiguiente, la protección de datos en el marco jurídico europeo se encuentra regulada en el art. 8 de la CDFUE al definir:

> toda persona tiene derecho a que los datos de carácter personal queden protegidos así como que los datos se traten de manera leal, para fines concretos y recibiendo el consentimiento de la persona concreta o en virtud de cualquier otro fundamento legítimo establecido por la ley[90].

Además de la CDFUE, destacamos los instrumentos legislativos vigentes en la UE en materia de protección de datos. En cuanto a las directivas, cabe hacer referencia en primer lugar a la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, del 24 de octubre de 1995 para garantizar la protección de los flujos de libertad de información dentro de la UE, considerada el principal instrumento de la legislación relativa a la protección de datos personales dentro de la UE. En esta directiva se regula la protección de la privacidad de los ciudadanos en correlación con el CEDH en su art. 10 al definir que:

> las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo [...][91].

---

[90] CDFUE, art. 8.

[91] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, art. 10.

Dicha directiva es exigible para todos los Estados Miembros teniendo como principios básicos los siguientes que se mencionan en el correspondiente artículo:

> Se establece unas condiciones generales para la licitud del tratamiento de datos personales y define los derechos de las personas cuyos datos son tratados, al tiempo que prevé la designación de autoridades nacionales de control independientes. De conformidad con la Directiva, el tratamiento de los datos personales está supeditado al consentimiento explícito del interesado, que ha de ser informado antes de que se proceda a dicho tratamiento[92].

En segundo lugar, encontramos la Directiva adoptada en el 2002 siendo la Directiva 2002/58/CE[93] modificada en el 2009 y cuyo objetivo principal fue el de reforzar con mayor precisión en el campo de las comunicaciones electrónicas complementando la Directiva de 1995. El derecho a la privacidad queda regulado en el art. 26 de la ya mencionada Directiva protegiendo la privacidad no sólo de las personas físicas sino de los intereses legítimos de las personas jurídicas.

También debemos recalcar el reglamento 45/2001 aprobado a finales del año 2000 por el Consejo y el Parlamento Europeo, para la protección de las personas físicas en lo que respecta al tratamiento de datos personales para las instituciones y los organismos comunitarios y a la libre circulación de esos datos. La Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, trata la protección de datos personales enmarcados en el marco de la cooperación policial y judicial en materia penal, siendo vinculante exclusivamente entre los estados miembros, autoridades y sistemas conexos dentro de la UE sin incluir los datos nacionales.

Una vez analizada la legislación en materia de protección de datos, vamos a citar determinadas sentencias consideradas relevantes en este ámbito debido a la posible vulneración ocasionada a dicho derecho. Respecto a las personas que gozan de dicha protección tenemos que mencionar la sentencia del TJUE *Volker und Markus Schecke y Eifert* en la que dispone:

---

92 DAVOLI A., La Protección de datos personales para el Parlamento Europeo, diciembre de 2013, apartado a.

93 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

el respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal […] se aplica a toda información sobre una persona física identificada o identificable[94].

Además, dicha sentencia es un claro ejemplo de vulneración de los artículos 7 y 8 de la CDFUE debido a que la injerencia consistía en publicar en una página web los datos nominales de los beneficiarios de la compañía agrícola, violando por tanto la Directiva 95/46/CE. [95] Debemos mencionar cómo también gozan de la protección de datos las personas jurídicas y no sólo las físicas como lo establece la sentencia Hoechst, de 21 de septiembre de 1989[96].

La protección de datos queda reforzada también en otras sentencias destacables como es la sentencia *Lindqvist*, de 6 de noviembre de 2003, que trata la cuestión relativa en materia de transferencia de datos en internet a terceros estados. A éstos se les exige que garanticen un nivel de adecuado de protección como se dispone en el art. 25 de la Directiva 95/46/CE y en el apartado 6 de dicha sentencia.[97] Esta sentencia también supone una vulneración de la Directiva de 1995. La sentencia mencionada la podemos poner en conexión con el nivel adecuado de protección que se exigía a los terceros estados en la transmisión de datos de los pasajeros en la adopción del Acuerdo de Puerto Seguro entre EEUU y la UE.

No podemos dejar de analizar la sentencia del TJUE, del PE contra el Consejo de la UE, de 30 de mayo de 2006, en materia de protección de las personas físicas relativo a la protección de datos. En este asunto *C-317/04*[98] el Parlamento Europeo solicita la anulación de la Decisión 2004/496/CE[99] relativa a la transferencia de los expedientes de los datos de pasajeros europeos al Departamento de Seguridad Nacional de los EEUU basado principalmente en la elección errónea del art. 95 del TUE como base jurídica para dicha Decisión como se afirma en la sentencia que:

esta Decisión no tiene por objeto y contenido el establecimiento y el funcionamiento del mercado interior, contribuyendo a la eliminación de obstáculos a la libre prestación de servicios, y no contiene disposiciones que persigan la consecución de este objetivo. En

94 STJUE, *Volker und Markus Schecke y Eifert,* 9 de noviembre de 2010,

95 *Op.cit;* CDFUE, apartado 66.

96 STJUE, Hoechst, de 21 de septiembre de 1989, apartado 20.

97 STJUE, Lindqvist, de 20 de mayo de 2003 apartado 6 y ss.

98 STJUE, PE contra Consejo de la UE, «Protección de las personas físicas en lo que respecta al tratamiento de datos personales, 30 de mayo de 2006.

99 Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004.

> efecto, su finalidad consiste en legalizar el tratamiento de datos personales impuesto por la legislación de Estados Unidos. Además, el artículo 95 CE no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo, dado que éste se refiere a tratamientos de datos que no están comprendidos en el ámbito de aplicación de la Directiva[100].

También, considera que ha habido vulneración del artículo 8 del CEDH del principio de proporcionalidad, de la exigencia de motivación y del principio de cooperación leal como se expone en el apartado 62 de la sentencia nombrada. Esta sentencia supuso el punto de partida para la creación del Acuerdo de Puerto Seguro entre EEUU y la UE. Aunque se haya firmado dicho Acuerdo veremos más adelante que se tienen que dar soluciones a las vulneraciones producidas por el conflicto de ley existente entre la normativa comunitaria y la legislación norteamericana en materia de protección de datos.

Por último, cabe hacer referencia a una sentencia que no ha sido resuelta por el TJUE sino por el TEDH en materia de protección de datos que es el caso *Leander* contra Suiza, en el que se consideró que además de la obtención y del almacenaje de datos, también la transmisión de los mismos o la negativa a los particulares a obtener información sobre los datos que los poderes públicos tengan sobre ellos es susceptible de suponer una vulneración del derecho a la privacidad[101]. Este caso lo ponemos en relación con la vulneración producida por las escuchas y almacenamiento masivo de datos producido por la NSA y por las agencias europeas de seguridad a través de los nuevos programas de espionaje sin dejar que los particulares puedan acceder a la información recopilada por éstas.

Como hemos podido observar a lo largo de este primer capítulo, las mayores vulneraciones son producidas por publicar datos personales en medios periodísticos o en internet vulnerando el art. 8 del CEDH y el art. 7 y 8 de la CDFUE. Las presuntas prácticas de vigilancia masiva sin justificación específica descritas previamente contravienen estos principios fundamentales. La UE y sus Estados miembros tienen la

[100] STJUE, PE contra Consejo de la UE, 30 de mayo de 2006, apartado 63 y ss.
[101] STEDH, Leander contra Suiza, de 26 de marzo de 1987.

obligación de proteger los datos personales de sus ciudadanos así como garantizar que cualquier transferencia internacional de datos respete los principios de las Directivas.[102]
Tomamos como punto de partida jurisprudencia de dichos tribunales en la que se haya vulnerado la privacidad de ciudadanos europeos para estudiar las futuras soluciones jurídicas. Por ello, una vez analizada la protección a la privacidad y las vulneraciones que se han cometido a la vista de las sentencias resueltas tanto en el ámbito del Consejo de Europa como en el marco de la UE, tratamos de proponer dos cuestiones fundamentales: por un lado expondremos determinadas soluciones para evitar las constantes vulneraciones producidas por los nuevos medios tecnológicos y por otro trataremos de responder a la pregunta: ¿Hacia dónde se dirige la Unión Europea en materia de protección de datos para lograr una mayor protección de la privacidad de las personas?

Respecto de la primera cuestión, en el ámbito de la UE, cabe destacar lo señalado por QUISPE al decir:

> el derecho a la intimidad se encuentra seriamente amenazado por la creciente capacidad que posee tanto el sector público como el privado de acumular y acceder a gran cantidad y variedad de información; la utilización de redes imperceptibles en las que circulan a gran velocidad, a bajo costo y sin ningún tipo de control información personal, importa la creación de una sociedad en la que todos nuestros actos y datos personales quedan registrados y son eventualmente comercializados[103].

Debido a esta nueva situación, LA RUE plantea determinadas soluciones debido a que:
"la vigilancia de las comunicaciones se considera un acto altamente invasivo que interfiere potencialmente con el derecho a la libertad de expresión y el derecho a la privacidad, amenazando las propias bases de una sociedad democrática"[104].

Por ello, LA RUE propone algunas soluciones[105] a los Estados. En primer lugar, la vigilancia de las comunicaciones debe estar regulada en los marcos legales siendo estos actualizados y su uso debe ser estricto cumpliendo el estándar de claridad y precisión

---

102 MORAES, C., *Sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos,* Documento de Trabajo para el PE.

103 SEGURA, A.A., *La protección al derecho a la intimidad y privacidad frente a las nuevas tecnologías*, En Revista del VII Congreso Iberoamericano de Derecho e Informática, Editora Perú, Lima 2000.

104 LA RUE F., Informe del relator especial para la promoción y protección del derecho a la libertad de opinión y de expresión, Consejo de Derechos Humanos, 20 de marzo de 2013, p.78.

105 *Op.cit;* PÉREZ DE NANCLARES., *Comentario a la CDFUE* […] p. 33 y ss.

siendo suficiente para que las personas puedan recibir notificación previa pudiendo prever su aplicación. Además, el uso de dicha vigilancia debe ser para fines exclusivamente legítimos y respetando el principio de proporcionalidad. También, se debe penalizar la vigilancia ilegal efectuada por los actores privados y públicos y el suministro de los datos de comunicación por parte de las entidades privadas al Estado debe estar claramente regulado por una autoridad independiente. Por último, también expone que se tienen que facilitar las comunicaciones privadas y seguras, incrementar el acceso público a la información sobre las amenazas a la privacidad y fundamentalmente avanzar en el marco internacional sobre la protección a la privacidad por el desarrollo de las nuevas tecnologías emitiendo un nuevo informe de protección a la privacidad para sustituir el Comentario General Nº16 de 1988.

Destacamos las propuestas que quiere adoptar el gobierno estadounidense para alcanzar soluciones a las vulneraciones producidas por su propia agencia de seguridad debido a las amenazas que durante estos últimos años EEUU ha estado recibiendo por parte de los Estados miembros de la UE. OBAMA expone diferente propuestas [106]. En primer lugar, la NSA va a seguir manteniendo los programas de recopilación de datos pero n o de forma masiva y sin la custodia ni el mantenimiento de ellos que estarán controlados o bien por una institución nombrada por la Administración de servicios de inteligencia o bien por una empresa tecnológica, obligándoles, por tanto, a adquirir una autorización judicial para tener acceso a ella. En segundo lugar, se reforma el Tribunal de Supervisión de Inteligencia Extranjera para comprobar si se ceden o no las autorizaciones judiciales para tener acceso a la información. Asimismo, los datos de las llamadas telefónicas se conservarán en las compañías de telefonía sin tener la obligación de conservar la información más que por un periodo establecido por ley[107]

Si se cumplieran las medidas mencionadas por parte de EEUU de vigilar y atender a la vigilancia realizada por la NSA y los EM de la UE llegaran a adoptar una mayor protección de la privacidad, se podrían evitar posibles vulneraciones a dicho derecho humano en el futuro.

---

[106] Artículo periodístico: Obama prepara el terreno para la inminente reforma de la NSA, 10 enero de 2014, http://internacional.elpais.com/internacional/2014/01/10/actualidad/1389375531_920093.html.
[107] http://actualidad.rt.com/actualidad/view/123342-obama-ley-restringir-nsa .

En cuanto a la segunda cuestión, la Unión Europea desde 2009 ha organizado sucesivas rondas de consultas públicas con el objetivo primordial de la creación de un Reglamento que sustituya a la Directiva 95/ 46/CE para alcanzar una aplicación más coherente de las normas de protección de datos en todos los Estados Miembros de la Unión. La finalidad que se pretende es alcanzar una protección de datos sólida y como se define en dicho informe:

> un marco legislativo sólido y coherente que cubre todas las políticas de la Unión, refuerza los derechos individuales, potencia la dimensión de mercado único de la protección de datos y reduce los trámites burocráticos engorrosos para las empresas[108].

A partir del 25 de enero de 2012, la Comisión Europea comenzó a realizar unas propuestas legislativas para adoptar una nueva directiva en materia de protección de datos para aumentar la protección de la privacidad y que los usuarios puedan tener más control sobre sus propios datos así como reducir los costes para las empresas. Debido a los avances tecnológicos y la distinta forma que los 28 estados miembros han aplicado la Directiva de 1995, es necesario un único acto legislativo para todos ellos. La Comisión propone:

> una Comunicación sobre los principales objetivos políticos de la reforma, una propuesta de Reglamento general para modernizar los principios consagrados en la Directiva sobre protección de datos de 1995, una propuesta de Directiva específica sobre el tratamiento de los datos personales en el marco de la cooperación policial y judicial en materia penal, y un informe sobre la aplicación de la Decisión Marco de 2008. El Parlamento y el Consejo debaten actualmente las propuestas de la Comisión, teniendo presentes tanto los intereses de los ciudadanos como los de las empresas[109].

Con todas estas herramientas jurídicas mencionadas consideramos que el derecho a la privacidad es un derecho humano que recibe protección en sucesivos tratados, convenios, sentencias y posturas doctrinales, aunque algunas propuestas están aún por consolidarse.

A continuación, pasamos a estudiar las posibles intervenciones del Estado y autoridades públicas en la privacidad de las personas para garantizar la seguridad, considerada un bien común y luchar contra el terrorismo.

---

[108] DAVOLI A., La Protección de datos personales para el Parlamento Europeo, diciembre de 2013, apartado 4.

[109] Ibid; *Supra* nota 106.

CAPÍTULO SEGUNDO: LAS LIMITACIONES AL DERECHO A LA PRIVACIDAD, EQUILIBRIO ENTRE UN DERECHO FUNDAMENTAL Y UN BIEN COMÚN.

1. Límites al derecho a la privacidad para garantizar la seguridad como bien común en el ámbito europeo:

Una vez analizado el apartado primero del art. 8 del CEDH, nos centramos en este capítulo segundo en estudiar las posibles limitaciones a dicho derecho. Realizamos la misma división que en el primer capítulo dividiéndolo en los dos ámbitos jurídicos principales el Consejo de Europa y la Unión Europea.

1.1 Consejo de Europa .

Las limitaciones para intervenir en la privacidad de las personas encuentran su regulación en el art. 8.2 del CEDH donde se menciona que únicamente habrá intervención por parte del Estado y de las autoridades públicas cuando:

> esté previsto por la ley y constituya una medida necesaria para una sociedad democrática para garantizar la seguridad nacional y pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás[110].

Nos centramos exclusivamente en el límite de "la garantía de la seguridad nacional y pública" debido a que las vulneraciones cometidas por el espionaje de la NSA, las agencias europeas y los Acuerdos han supuesto grandes violaciones a ciudadanos europeos por la ilegal forma de vigilancia al recopilar información de datos a compañías y embajadas europeas. La intervención en la privacidad se entiende que es lícita cuando se garantice la seguridad nacional y pública. A raíz de las vulneraciones mencionadas en nuestro capítulo introductorio, la mayoría de los estados han aumentado la seguridad en los aeropuertos y en otros lugares de tránsito con la función principal de recoger los datos biométricos de los pasajeros[111] para verificar si esas personas podrían ser consideradas terroristas.

---

[110] CEDH de 1950, art. 8.2.

[111] Mención al Acuerdo de Puerto Seguro.

Es necesario estudiar el significado de: "esté previsto por la ley y constituya una medida necesaria para una sociedad democrática" mencionado previamente, siendo común a todas las limitaciones que se exponen en dicho artículo. El principio de que las injerencias por parte de las autoridades públicas sean lícitas se recoge en la sentencia Mikulic contra Croacia, de 2002[112] en la que el Tribunal dispone en su apartado 53 que las injerencias deben estar previstas legalmente. También, la sentencia Malone contra Reino Unido, de 2 de agosto de 1984, regula el requisito de estar previsto por la ley al disponer:

> la ley debe emplear los términos suficientemente claros para indicar a todos de manera adecuada las circunstancias y las condiciones en las que se habilita a los poderes públicos para realizar atentados secretos al derecho al respeto de la vida privada y de la correspondencia[113].

Otras sentencias del TEDH se han centrado en este asunto como el caso Rotaru contra Rumania[114] y por el caso Amman contra Suiza resuelto por el TEDH, en el que se reitera la postura acerca de la expresión previsto por la ley se impone no solamente a que la medida adoptada tenga base en el derecho interno sino que se dirija también a la calidad de la ley[115].

Respecto del segundo elemento del art. 8.2 la sentencia Klass y otros contra Alemania da una aproximación a cómo deberían de ser las medidas necesarias para una sociedad democrática al decir:

> El Tribunal debe convencerse de la existencia de garantías adecuadas y suficientes contra los abusos […] depende de todas las circunstancias que envuelven el caso, por ejemplo, la naturaleza, el alcance y la duración de las eventuales medidas, las razones requeridas para ordenarlas, las autoridades competentes para autorizarlas, ejecutarlas y el tipo de recursos previstos por el derecho interno[116].

Junto con la sentencia mencionada, encontramos la sentencia Gillow[117] que también adopta una aproximación de lo que se entiende por medida necesaria para permitir la intervención a las autoridades públicas en la privacidad de los ciudadanos al definir que una medida necesaria: "implica una injerencia basada en una necesidad social imperiosa

---

112 STEDH, Mikulic contra Croacia, 2002, ap.53.

113 STEDH Malone contra Reino Unido, 2 de agosto de 1984.

114 STEDH, Rotaru contra Rumania, de 4 de mayo de 200.

115 STEDH, Amman contra Suiza, 2000, ap. 87.

116 STEDH, Klass y otros contra Alemania, 6 de septiembre de 1978, ap. 50.

117 Veáse también la STEDH, Golder, de 21 de febrero de 1975, ap.34.

y sobre todo proporcionada al fin legítimo perseguido"[118]. Las injerencias por parte de las agencias de espionaje estadounidenses y europeas y las revelaciones de Snowden no se fundamentan en medidas que se consideren necesarias para una sociedad democrática y tampoco cumplen el objetivo principal de nuestro trabajo de buscar el equilibrio entre el ejercicio por el individuo del derecho que le garantiza el párrafo primero del art. 8 y la necesidad, según el apartado segundo, de imponer una vigilancia secreta para proteger a la sociedad democrática en su conjunto.

Una vez se ha concretado la importancia de que las injerencias deben estar previstas por la ley y de que las medidas que se adopten han de ser necesarias para una sociedad democrática, se examina el límite que consideramos junto con la mayor parte de la doctrina y de la postura adoptada por el TEDH para poder intervenir en la privacidad de las personas con el fin de proteger la seguridad nacional y la seguridad pública.

Determinadas sentencias resueltas por el TEDH han permitido que se hayan producido injerencias en el derecho humano para garantizar la seguridad bien nacional o pública. Encontramos el caso *Leander* contra Suecia, de 26 de marzo de 1987, en el que el TEDH afirma que no existe violación de la privacidad por cumplirse los límites reconocidos en el apartado segundo de dicho artículo. En este supuesto, el sistema sueco de control de personal persigue uno de los fines legítimos del mencionado artículo: la protección de la seguridad nacional. El TEDH confirma la necesidad de recopilar la información y ponerla a disposición de la policía especial cuya única finalidad es la prevención de delitos contra la seguridad nacional. La seguridad nacional queda definida en dicha sentencia como:

> Para preservar la seguridad nacional, los Estados contratados tienen innegablemente necesidad de Leyes que habiliten a las autoridades internas competentes a obtener y a registrar en ficheros secretos informaciones sobre personas, y a utilizarlas cuando se trate de evaluar la aptitud de los candidatos a puestos importantes desde el punto de vista de dicha seguridad[119].

El Tribunal junto con la Comisión Europea concluyen que las garantías que rodean el sistema de control cumplen con los requisitos del art.8.2 al estar el gobierno sueco en su derecho de considerar que en este supuesto concreto, los intereses de la seguridad nacional prevalecen sobre los intereses de los individuos del demandante.

---

[118] STEDH, Gillow, de 24 de noviembre de 1986, ap.15.

[119] STEDH, Leander contra Suecia, 26 de marzo de 1987, ap. 4.

Si comparamos esta sentencia con las vulneraciones expuestas por la NSA llegamos a la conclusión que la agencia nacional de seguridad ha utilizado información de datos personales europeos no para prevenir la seguridad nacional ni para evitar el terrorismo, ya que la información recopilada era masiva y no se identificaba con claridad.

También, cabe hacer mención al caso Murray contra Reino Unido, de 28 de octubre de 1994, al considerarse una sentencia resuelta por el TEDH en la que tampoco se produce una vulneración a la privacidad por cumplir con el límite reconocido en el apartado segundo del art. 8 donde dispone en la sentencia lo siguiente que: "los registros domiciliarios, retenciones de personas e incluso toma de fotografías como parte de un operativo son necesarias para combatir el terrorismo"[120].

Cabe destacar la postura de LA RUE en el tema de la seguridad nacional ya que no sólo define el derecho humano de privacidad, sino que además permite que se adopten ciertas restricciones a dicho derecho y que también se lleguen a utilizar ciertas medidas de espionaje por los estados cuando concurran circunstancias consideradas por este autor excepcionales como la administración de justicia criminal, la prevención de crímenes[121] o la prevención contra el terrorismo. Estas circunstancias deben de cumplir con el CEDH junto con las leyes internas de cada estado y siempre respetando el principio de proporcionalidad[122].

Junto con LA RUE, es importante hacer referencia para garantizar la seguridad nacional y la seguridad pública así como también luchar contra el terrorismo a las Directrices del Consejo de Europa sobre los derechos humanos y la lucha contra el terrorismo. En estas directrices se dispone que para luchar contra ataques terroristas, la recolección y el tratamiento de los datos por cualquier autoridad competente en materia de seguridad

120 STEDH, Murray contra Reino Unido, de 28 de octubre de 1994, ap. 23. Véase también la STEDH: *Bosphorus* contra Irlanda, 30 de junio de 2005, en la que se trata de combatir contra el terrorismo internacional.

121 Véase STEDH, *Segerstedt-Wiberg* y otros contra Suecia, 6 de junio de 2006, que trata la cuestión de combatir los crímenes de guerra.

122 LA RUE, F., del relator especial para la promoción y protección del derecho a la libertad de opinión y de expresión, Consejo de Derechos Humanos, 20 de marzo de 2013, p.59.

[123]de la esfera personal sólo podrá intervenir en la vida privada de las personas cuando se cumplan tres elementos principales: "que están regulados por disposiciones apropiadas en derecho interno, están en proporción con el objetivo por el que han sido previstos y son susceptibles de control por una autoridad externa independiente".[124]

1.2 Unión Europea.

En este último punto, estudiamos las limitaciones existentes en el ámbito jurídico de la UE. A diferencia de lo que ocurre con el art. 8.2 del CEDH que regula las limitaciones a las interferencias en la esfera del derecho humano de privacidad, el art. 7 de la CDFUE no los regula en ningún apartado y por ello, conforme al art. 52.3 de la CDFUE, a éste precepto se le tiene que dar el mismo sentido que el art. 8.2 que la jurisprudencia ha resuelto a través del TEDH.

La seguridad, considerada la limitación principal en nuestro trabajo para justificar las intromisiones en la esfera privada, se regula en el art. 6 de la CDFUE al disponer: " toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, salvo en los casos siguientes y con arreglo al procedimiento establecido por la ley"[125].

El TJUE ha resuelto diversas sentencias en materia de seguridad como límite a la vulneración del derecho a la privacidad. En primer lugar, mencionamos la sentencia *Carpenter,* de 11 de julio de 2002, en la que ya se adoptaban los límites del art. 8.2 del CEDH.[126] Para que la acción limitadora fuera correcta tenía que cumplir los siguientes requisitos: se exigía la defensa de un interés general, no afectar a la esencia del derecho y en todo caso, respetar la proporcionalidad de la medida. [127] Conforme a esta situación, es importante poner en conexión estos requisitos con las vulneraciones cometidas por la transmisión masiva de datos y en concreto con los datos de información financiera.

---

123 Hágase referencia a las agencias de seguridad europeas mencionadas en el capítulo preliminar que cedían información masiva e indiscriminada a la NSA.

124 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Los derechos Humanos, el Terrorismo y la Lucha contra el Terrorismo, Folleto informativo nº 32, p. 49-50.

125 CDFUE, art.6.

126 STJUE, Carpenter, 11 de julio de 2002, ap.42.

127 Véase también las sentencias: STJUE, Scrhader, 11 de julio de 1989, ap.15 y la STJUE Alemania c. Comisión, 8 de abril de 1992, ap.23.

VARA expone que al recopilar datos financieros se puede luchar contra el terrorismo y garantizar la seguridad obteniendo datos como los nombres, direcciones y/o números de facturas correspondientes a las personas. Este autor expone que :

> En estas circunstancias la transferencia de datos de mensajería financiera a los Estados Unidos constituye una vulneración de los principios fundamentales en los que se basa la legislación de la UE en materia de protección de datos a saber los principios de necesidad y de proporcionalidad[128].

Por ello, en la transmisión masiva de datos entre EEUU y la UE se vulnera el principio de proporcionalidad mencionado en la sentencia anterior. Dicho Acuerdo de Puerto Seguro se diferencia del *Total Information Awareness (TAI)* cuyo objetivo principal es combatir contra los ataques terroristas.

En segundo lugar, encontramos el caso Schwarz resuelto por el TJUE, de 17 de octubre de 2013, en el que aunque el señor Schwarz argumenta en la sentencia la vulneración de su privacidad y de la protección de datos, el TJUE concluye que el tomar las impresiones dactilares no suponía una vulneración de los art. 7 y 8 de la CDFUE al disponer que:

> la toma consiste únicamente en captar la impresión dactilar de dos dedos, los cuales están normalmente a la vista de los demás, de modo que no se trata de una operación que revista un carácter íntimo […]
> e implica que tal conservación puede reducir el riesgo de falsificación de pasaportes y facilitar la tarea de las autoridades encargadas de examinar la autenticidad de los mismos en las fronteras.[129]

En la primera parte de la cita se confirma que no existe una vulneración al derecho de privacidad dado que la operación no reviste un carácter íntimo y en la segunda parte hace referencia a la necesidad de adoptar dicha medida para garantizar la seguridad y evitar que las personas que viajen no utilicen pasaportes falsificados. Cuando éste sea el objetivo entonces sí que se entenderá justificada la intervención a la privacidad.

Por ello, consideramos que es lógico que cuando se quiera luchar contra el terrorismo se establezcan ciertas limitaciones a los derechos de los interesados. Así, como determina VARA:

> se prevé que la revelación a una persona de sus datos personales podrá limitarse en las circunstancias que prevea la legislación nacional "para salvaguardar la prevención, detección, investigación o persecución de delitos, así como para proteger el orden público o

---

128 *Op.cit*; VARA, J.S, "*La transferencia de datos […]",* p.15.

129 STJUE, Schwarz, 17 de octubre de 2013, ap. 48 y 41.

la seguridad nacional, teniendo debidamente en cuenta los intereses legítimos del interesado[130].

Junto con las sentencias mencionadas previamente acerca de la seguridad nacional y la seguridad pública cabe hacer referencia al Acuerdo de transmisión de datos financiero entre EEUU y la UE en el que en dicho Acuerdo en su art. 7 se expone que aunque como norma general cuando se transmite información a terceros estados se requiere el consentimiento con la excepción que:

> En virtud de la cual no es preciso obtener el consentimiento previo del Estado afectado" si el compartir datos es esencial para la prevención de una amenaza grave e inmediata contra la seguridad pública de una parte del presente Acuerdo, un Estado miembro o un tercer país.[131]
>
> El Departamento del Tesoro de los Estado Unidos solicitará […] la puesta a disposición de los datos para prevención, investigación, detección o persecución del terrorismo o de la financiación de ésta[132].

Cuando se den estas circunstancias, las autoridades de los EEUU no necesitan el correspondiente consentimiento porque se está cumpliendo uno de los límites principales que es la seguridad pública. Por ahora, las transmisiones de datos entre EEUU y la UE no han cumplido esta limitación y continuamos pensando que se ha vulnerado la privacidad de miles de ciudadanos europeos.

Para evitar dichas vulneraciones se podrían adoptar algunas soluciones que compartimos junto con VARA[133] como el desarrollo por parte de la UE de un sistema parecido al TFTP norteamericano evitando con ello la filtración masiva de información. Este sistema permitiría que las autoridades europeas pudieran realizar una selección específica de la solicitud de datos para transmitir exclusivamente a las autoridades norteamericanas informaciones selectivas y no masivas. Con esto, se podría llegar a contribuir la lucha contra la financiación del terrorismo dentro de la UE y reducir de manera significativa el volumen de datos que es transferido a los EEUU. Es fundamental considerar el trabajo del EUROPOL[134] , agencia europea que se dedica a clasificar y reorganizar información relativa a amenazas contra los ciudadanos de la UE. La E-3440/02 afirma que:

> para las relaciones con los Estados Unidos […] Dichos datos sólo se intercambian en caso de que existan peligros para la vida de una persona, bajo la responsabilidad del director de

130 Ibid; *Supra* nota 128 p. 18.

131 Acuerdo Switft entre EEUU y la UE, 1 de agosto de 2010, art. 7.

132 Ibid; *Supra* nota 125, art.4 del Acuerdo.

133 *Op.cit;* VARA, J.S, La transferencia de datos […], p. 20.

134 Véase su significado: agencia de seguridad de la UE.

> Europol y la supervisión del Consejo de Dirección y la base jurídica para la transmisión excepcional de datos personales a los Estados Unidos, de ser ésta absolutamente necesaria para salvaguardar los intereses fundamentales de los Estados miembros o prevenir un peligro inminente de comisión de delito[135].

Como recoge NANCLARES, el verdadero reto de la UE con respecto a la privacidad y a la protección de datos es lograr el necesario equilibrio entre las medidas necesarias para abordar eficazmente las amenazas contra el terrorismo internacional y las delincuencias organizadas. La protección de datos: "se tendría que garantizar *ad intram* en los 28 Estados Miembros que lo componen, pero también habrá de hacerlo *ad extram* prestando adecuada protección a los datos personales que facilite a terceros Estados, como por ejemplo, a Estados Unidos". También, se sustenta que la protección de datos se extienda de manera efectiva al ámbito de la PESC y la Política Europea de Seguridad y Defensa[136].

2. Conclusiones:

El presente trabajo no trata de priorizar el derecho humano a la privacidad frente a la seguridad o viceversa, sino de exponer la vulneración a la privacidad de los ciudadanos europeos que se ha producido por parte de la NSA y de las agencias secretas europeas, principalmente la británica GCHQ, como reveló Edward Snowden en sus acusaciones contra dichas agencias. Las violaciones producidas se han difundido a través de datos que fueron proporcionados por periódicos como *The Guardian*, *The Washington Post o Der Spiegel* que informaron sobre los datos masivos que recopilaban las agencias. La información adquirida no recogía datos para defender la seguridad nacional o luchar contra el terrorismo, sino que como se ha demostrado consistía en información relativa a la vida privada de millones de ciudadanos, de primeros ministros como David Cameron o Ángela Merkel, embajadas y organizaciones no gubernamentales como UNICEF o Médicos del Mundo. Es importante mencionar cómo han sido adquiridas estas revelaciones: coaccionando a empresas, robando claves, interviniendo en escuchas privadas telefónicas y utilizando cables para adquirir dicha información vía internet. Además, la utilización de los programas PRISM o *cloud computing* suponen una

---

135 MARCI C., Intercambio de datos personales entre Europol y los Estados Unidos, Diario Oficial de la Unión Europea. , Consejo de 2 de diciembre de 2002.

136 *Op.cit*; NANCLARES., Carta de los Derechos Fundamentales de la Unión Europea, p.242.

vulneración a la privacidad por no respetar los principios de privacidad reconocidos en el Acuerdo de Puerto Seguro.

Se ha querido explicar la importancia de la transmisión de datos entre la UE y los EEUU destacando los dos Acuerdos más relevantes en esta materia: el Acuerdo de Puerto Seguro y el Acuerdo *SWIFT*. Aunque se está trabajando en adoptar soluciones concretas, ambos acuerdos suponen un apoyo entre EEUU y la UE para estimular las relaciones entre ambos y conseguir el equilibrio primordial entre proteger la privacidad y a su vez luchar contra el terrorismo, garantizando la seguridad nacional.

Nos hemos centrado en el ámbito jurídico europeo debido a las vulneraciones sufridas por personas que se encuentran protegidas por dicho marco, sin descartar la importancia de la DUDH y otros tratados específicos que dotan de protección a la privacidad como un derecho humano. Tanto el art. 8 del CEDH como el art. 7 de la CDFUE han sido principales en nuestro trabajo al analizar los elementos que lo componen, y comprobar por medio de sentencias tanto del TEDH[137] como del TJUE[138] las injerencias cometidas para posteriormente, indagar soluciones a las violaciones producidas por el espionaje y los nuevos medios tecnológicos. Es importante recalcar que en el ámbito de la UE existen pocas sentencias resueltas por el TJUE en dicha materia ya que se ha producido una remisión de la CDFUE al CEDH por medio del art. 52.3 de dicha Carta.

La transmisión de datos ha sido esencial en nuestro estudio dado que las vulneraciones explicadas en el capítulo preliminar son producidas bien por la adquisición de datos privados o bien por la transmisión de éstos por agencias europeas a la NSA. Los instrumentos legales vigentes en la UE son la Directiva del año 1995 y 2002 y el Reglamento 45/2001. En este ámbito ha habido varias sentencias en las que se ha vulnerado principalmente la Directiva de 1995 a destacar la sentencia del PE contra el Consejo de la UE de 2006 en materia de protección de datos de las personas físicas.

Se ha tomado como punto de partida las sentencias resueltas por ambos tribunales para adoptar determinadas soluciones a las vulneraciones de dicho derecho. Compartimos las propuestas adoptadas por LA RUE ya mencionadas en el presente trabajo siendo

[137] A destacar STEDH como Kopp contra Suiza o Airey contra Irlanda.
[138] A destacar STJUE: Carolina contra Alemania y el caso IPI.

principal la actualización de los marcos legales que regulen la vigilancia de las comunicaciones y el consentimiento de los ciudadanos para permitir que su información sea utilizada o transmitida. También, la vigilancia debe ser utilizada exclusivamente para fines legítimos, proporcionados y para evitar futuras amenazas terroristas. A principios de 2014 el gobierno estadounidense debido a las amenazas recibidas de los Estados miembros de la UE, pretende reformar el sistema de recopilación de información de la NSA, adoptando mayores medidas de protección de la información recopilada. Por último en el ámbito europeo, ha sido cuestión de debate desde 2012 la reforma de la actual Directiva de protección de datos para modernizarla y conseguir una mayor protección.

Se concluye que la única posibilidad en la que se permitiría la intercepción en la privacidad de las personas es si se cumplen los límites del art.8 del CEDH, siendo la seguridad nacional y pública las limitaciones escogidas en nuestro trabajo. Tras el estudio de la jurisprudencia, se ha llegado a la conclusión que sólo cuando se utilicen datos para proteger la prevención, detención o persecución del orden público o seguridad nacional se podrá intervenir en la vida privada de las personas. Como hemos visto a lo largo del trabajo se ha justificado que la NSA, las agencias de espionaje europea y las revelaciones de Snowden no obtienen la información para luchar contra el terrorismo ni para garantizar la seguridad nacional o pública al no acogerse a las limitaciones del mencionado artículo.

Por ello afirmamos que debido a las vulneraciones cometidas por el espionaje, el concepto de privacidad que adoptamos es el expuesto por PRATS que entiende la privacidad como libertad positiva. Dicho autor afirma que se tiene que ejercer un mayor control sobre los datos privados de las personas para conseguir una mayor protección a su privacidad y para evitar violaciones de su libertad en el futuro. Todo lo manifestado anteriormente no debe soslayar la atención de los Estados a la seguridad de sus ciudadanos, siendo el terrorismo la línea roja que permitiera la interferencia en la vida privada de los individuos para así proteger un bien común. La libertad y la vida privada debe por tanto ligarse con la defensa no sólo frente a una alteración de la seguridad de los Estados sino también frente a cualquier violación injusta del derecho humano a la privacidad y a la libertad individual.

BIBLIOGRAFÍA.

MONOGRAFÍAS:

AGUSTINA, J.R., (Dir) *Tendencias en prevención del delito y sus límites, Privacidad y dignidad humana frente al uso de las nuevas tecnologías*, Madrid, EDISOFER S.L agosto de 2010.

ETZIONI, A. AGUSTINA, J.R. (Dir), *Los límites de la privacidad*, EDISOFER S.L, 2012.

Jornadas sobre protección de la privacidad, telecomunicaciones e internet, Agencia de Protección de datos junto con la Universidad Pública de Navarra, 22 y 23 de junio de 2000.

VARA J.S. MARTÍN y PÉREZ DE NANCLARES J. (Coord), *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*, *"El acuerdo SWIFT con Estados Unidos: génesis, alcance y consecuencias" p. 355-380.*

ARTÍCULOS Y REVISTAS**:**

ÁLVAREZ UGARTE, R., *El caso Snowden y la democracia en disputa,* NUEVA SOCIEDAD Nº 247, (2013), ISSN 0251 3552, p.28-36.

BALLESTEROS MOFFA, L.A*., Hacía un difícil equilibrio entre privacidad y seguridad*: *la conservación de datos en las comunicaciones electrónicas y la transferencia de datos de pasajeros por las compañías aéreas*., Civitas, Revista Española de derecho administrativo, (2008), ISSN 0210 8461 Nº 137, p. 31-55.

CASTILLO JIMÉNEZ, C., *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*, Derecho y Conocimiento vol.1 ISSN 1578 8202, p. 35-48.

DAVARA RODRÍGUEZ, M.A., *Intimidad, protección de datos y seguridad: Un difícil equilibrio*, Diario La Ley (2009) ISSN 1138-9907. Nº7276, p.1384-1387.

DIDIER, B. A.A.V.V., *Fighting Cyber crime and protecting privacy in the cloud*, Study for the European Parliament, PE 462.509.

ELLIOT SEGURA, A.A., *La protección al derecho a la intimidad y privacidad frente a las nuevas tecnologías*, en Revista del VII Congreso Iberoamericano de Derecho e Informática, Editora Perú, Lima 2000.

FRIEDMAN, T.L., *Hacker Lesson: Wired citizens Needs Government*, 16 of February 2000.

MANGAS, M. A., (Dir) y GONZÁLEZ ALONSO L. (Coord), *Carta de los Derechos Fundamentales de la Unión Europea, Comentario artículo por artículo, "* p. 195-243.

MEYERS, D., *Los derechos inalienables*, Alianza Editorial, Madrid, 1988 Columbia University Press, 1985. Trad. E. Beltrán, p. 13.

MORALES PRATS, F., *La tutela penal de la intimidad: privacidad e informáti*ca, ed. Destino, Barcelona, 1984, p. 15 y ss.

POLONETSKY., *Privacy and the Age of Big Data, A time for big decisions,* Standford Law Review.

PRASOW, A., *US*: *Surveillance practice violates Rights*, Report for Human Rights Watch, 12 of march 2014.

SOLOVE, J., *Nothing to Hide*, *The false tradeoff between privacy and security*, Yale University Press, 2011.

SCHNEIDER, F., *Intergovernmental organizations*, American University Washington College of Law, Human Rights Brief, p.2.

TRIVIÑO, J.L., *Derechos Humanos, Relativismo y protección jurídica de la moral en el Convenio Europeo de Derechos Humanos,* p. 469-490.

VARA, J.S., *La transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos*, Cátedra Telefónica de la Universidad de Salamanca, p. 7-22.

OTROS DOCUMENTOS:

CARRERA, S. ELSPETH GUILD y PARKIN J., *Who will monitor the spies*?, Report for the Centre for European Policy Studies, 8 January 2014.

DAVOLI, A., *La Protección de datos personales* para el Parlamento Europeo, diciembre de 2013.

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (TFTP), Diario Oficial de la Unión Europea, 2010, C355/02.

DIDIER, B. A.A.V.V., *Fighting Cyber crime and protecting privacy in the cloud*, Study for the European Parliament, PE 462.509.

Directorate General for Internal Policies, *The US surveillance programmes and their impact on EU citizens´fundamental rights*, Policy Department citizen´s rights and constitutional affairs, Report for the European Parliament, 2013, p. 4-33.

LA RUE, F., Informe ante el Consejo de Derechos Humanos de Naciones Unidas: *Incidencia de la Vigilancia Estatal de las Comunicaciones en el Derecho a la Privacidad y el Derecho a la Libertad de Expresió*n, 2012.

LA RUE, F., *Informe del relator especial para la promoción y protección del derecho a la libertad de opinión y de expresión*, Consejo de Derechos Humanos, 20 de marzo de 2013, p.59.

MARCI, C., *Intercambio de datos personales entre Europol y los Estados Unidos*, Diario Oficial de la Unión Europea., Consejo de 2 de diciembre de 2002.

MORAES, C., *Sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos,* Documento de Trabajo para el PE, 11 de diciembre de 2013.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Los derechos Humanos, el Terrorismo y la Lucha contra el Terrorismo*, Folleto informativo Nº 32, p. 49-50.

Reporters without Borders, *Enemies of the Internet 2014, " Europe and Central Asia" p. 13. "Americas, NSA: National Security Agency"* p.18-20.

SITIOS DE INTERNET:

Privacy International. Una guía de privacidad para hispanohablantes. https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/informacion-general-sobre-privacidad. (consultado el día 5 de febrero de 2014)

<http://elpais.com/elpais/2014/01/11/opinion/1389461699_383984.html> (consultado día 20 enero de 2014)

<http://www.elmundo.es/tecnologia/2013/10/15/525d19030ab7408e758b4577.html> (consultado el día 6 de febrero de 2014)

<http://internacional.elpais.com/internacional/2013/06/29/actualidad/1372527016_180298.html> (consultado el día 15 febrero de 2014)

<http://internacional.elpais.com/internacional/2013/06/29/actualidad/1372527016_180298.html> (consultado el día 15 de febrero de 2014)

<http://internacional.elpais.com/internacional/2013/12/20/actualidad/1387553750_569745.html >(consultado el día 13 de febrero de 2014)

<http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance> (consultado el día 11 de febrero de 2014)

<http://www.nytimes.com/2013/08/08/usbroader-sifting-of-data-abroad-is-seen-by-nsa-html?pagewanted=1&hp> (consultado el día 11 de febrero de 2014)

<http://washigtonpost.com/politics/federal_government/report-surveillance-court-ruling-allowed-nsa-search-of-domestic-email/2013/09/08/4d9c8bb8-18c0-11e3-80ac-96205cacb45a story.html> (consultado el día 12 de febrero de 2014)

<http://internacional.elpais.com/internacional/2014/01/10/actualidad/1389375531_920093.html> (consultado el día 10 de marzo de 2014)

http://actualidad.rt.com/actualidad/view/123342-obama-ley-restringir-nsa
(consultado el 25 de marzo de 2014)

<http://internacional.elpais.com/internacional/2014/03/29/actualidad/1396104499_199182.html> (consultado el 30 de marzo de 2014)

DECLARACIONES, CONVENIOS Y LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UE:

Carta de los Derechos Fundamentales de la Unión Europea, publicado en el DOUE, 30 de marzo de 2010, C-83/02.

Convenio Europeo para la protección de Derechos Humanos y las Libertades Fundamentales, Roma 4 de noviembre de 1950, publicado en el BOE número 243, de 10 de octubre de 1979.

Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familias, aprobada por la Asamblea General por Resolución 45/158 del 18 de diciembre de 1990.

Convención de los Derechos del Niño, adoptada y abierta a la firma, ratificación e incorporación por la Asamblea General por Resolución 44/25 del 20 de noviembre de 1989, entrada en vigor 2 de septiembre de 1990.

Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Resolución 217 A (III) de la Asamblea General el 10 de diciembre de 1948

JURISPRUDENCIA UTILIZADA:

STEDH, Alkaya contra Turquía, 9 de octubre de 2012, Nº 42881/06, párr.32 (Aranzadi-Westlaw)

STEDH, Pretty contra Reino Unido, Nº. 2346/02, párr. 61.

STEDH, K.U. contra Finlandia, de 2 diciembre 2008, Nº 2872/02. (Aranzadi-Westlaw)

STEDH, Kopp contra Suiza, de 25 marzo 1998, Nº 2001/407, párr.64 y ss. (Aranzadi-Westlaw)

STEDH, Airey contra Irlanda, de 9 de octubre de 1979, Nº 6289/73, párr. 32. (Aranzadi-Westlaw)

STEDH Marckx contra Bélgica, 13 de junio de 1979, Nº 6833/74, párr.31.

STEDH, Amman contra Suiza, 2000, Nº 2000/87, párr. 87.

STEDH, Klass y otros contra Alemania, 6 de septiembre de 1978, Nº 5029/71 párr. 50.

STEDH, Gillow, de 24 de noviembre de 1986, Nº 9063/80, párr.15

STEDH, Murray contra Reino Unido, de 28 de octubre de 1994, párr.. 23.

STJUE, Carolina contra Alemania, 24 de junio de 2004, párr. 57. (Comentario Carta de Derechos Fundamentales de la Unión Europea)

STJUE, *Volker und Markus Schecke y Eifert,* 9 de noviembre de 2010, C-92/09.

SJUE, Hoechst, de 21 de septiembre de 1989, C-94/00, párr. 20.

STJUE, Lindqvist, de 20 de mayo de 2003, C-101/01 párr. 6 y ss.

STJUE, PE contra Consejo de la UE, Protección de las personas físicas en lo que respecta al tratamiento de datos personales, 30 de mayo de 2006. C-317/04.

STJUE, Carpenter, 11 de julio de 2002, párr.42. (Comentario de la Carta de los Derechos Fundamentales)