¿CAZADOR O PRESA EN LA TELARAÑA DEL TERROR?: LA UE EN LA LUCHA CONTRA EL CIBERTERRORISMO

HUNTER OR PREY IN THE WEB OF TERROR? THE EU IN THE FIGHT AGAINST CYBERTERRORISM

Alejandro SÁNCHEZ FRÍAS[*]
Becario de Investigación (FPU) en Derecho Internacional Público
Universidad de Málaga

RESUMEN

El uso de las nuevas tecnologías ha avanzando de forma imparable en las últimas décadas, y con ello el uso que hacen de ellas los grupos terroristas. El caso más claro es el de Internet, plataforma que es usada de forma cada vez mayor para la comisión de actos delictivos. De forma contraria a la que pudiera pensarse, el mayor uso de Internet por estos grupos no es para realizar ataques directos contra infraestructuras críticas sino para colgar contenidos ilegales en la red. Es por ello que el desarrollo de medidas en el ámbito de la seguridad es esencial para eliminar los actos terroristas en Internet. El papel que juega la UE para ayudar a combatir esta amenaza global es esencial dadas las competencias que tiene atribuidas en materia del Espacio de Libertad, Seguridad y Justicia.

PALABRAS CLAVE: terrorismo, ciberterrorismo, ciberespacio, reclutamiento, adiestramiento, financiación, propaganda, seguridad, libertad, derechos humanos, conservación de datos.

[*] Los resultados de este trabajo fueron presentados en ponencia en "II Seminario Internacional UC3M sobre Criminalidad Organizada Transnacional y Terrorismo" con las ayudas para asistencia a congresos del Plan Propio de Investigación de la Universidad de Málaga.

1. Introducción

El terrorismo no es una amenaza de reciente creación. ¿Por qué entonces realizar una investigación sobre un tema que viene ya desde antiguo y tratado en innumerables ocasiones? La respuesta subyace en la propia evolución de las nuevas tecnologías que ha dotado tanto de nuevas comodidades a la sociedad en general como de nuevas armas a esta amenaza de dimensiones globales. Nuestro objetivo es por tanto profundizar en la lucha contra una actuación terrorista concreta: la que se realiza en el ciberespacio. Los distintos actores nacionales y supranacionales que aquí intervienen son muchos, siendo uno de los más relevantes la Unión Europea con su labor armonizadora.

Son dos por tanto las reducciones con que se plantea esta investigación: la primera de terrorismo a ciberterrorismo y, la segunda, de todos los actores implicados a únicamente la Unión Europea. Pero ello sigue sin ser suficiente para elaborar un trabajo de reducidas dimensiones. Por tanto, realizaremos una tercera concreción: trataremos no ya el ciberterrorismo en todas sus acepciones, sino que excluiremos la vertiente de ataques directos a través de la red. Ello nos permitirá centrar el enfoque de nuestro trabajo no ya en la vertiente militar, más restringida competencialmente, sino en la seguridad.

La realidad a la que se enfrenta esta investigación no es, por tanto, la totalidad de los usos terroristas en internet, sino únicamente la lucha contra los contenidos terroristas presentes en la red. Con ello podemos ya plantear los tres interrogantes que intentaremos resolver a lo largo de las siguientes páginas: ¿cuáles son las formas de contenidos terroristas en Internet?, ¿qué instrumentos jurídicos y políticos posee la Unión Europea para combatir esta amenaza?. Y, en un tono más personal y *pro futuro*, ¿cuáles son los logros y deficiencias de estas medidas y la adecuación de las propuestas planteadas? En consecuencia, el objeto del presente trabajo será presentar y analizar los instrumentos jurídicos de que puede dispone a Unión Europea en la lucha contra el ciberterrorismo, dada la realidad actual del terrorismo en Internet.

El método a seguir para aportar respuestas a estas incógnitas es de gran sencillez en su planteamiento. Primero se expondrán cuál es el uso que da a Internet el grupo terrorista, con los límites señalados, y las ventajas que ello le aporta. Una vez

identificada la realidad a la que nos enfrentamos, trataremos los documentos jurídicos y políticos elaborados en el seno de la Unión Europea. Para ello nos centraremos en qué instrumentos sobre el ciberespacio son aplicables al terrorismo y en aquellos otros sobre terrorismo que pueden acoplarse en el ciberespacio. Mas allá de presentar un análisis exhaustivo de todos y cada uno de ellos, proporcionaremos una visión inicial respecto a qué instrumentos proporcionan cobertura al incremento de la seguridad frente a las actuaciones terroristas en Internet, y cuáles son las lagunas conforme a la realidad existente expuesta en el primer apartado. Estas "lagunas" deben entenderse no sólo en cuanto a déficits de seguridad, sino también en cuanto a falta de protección de los derechos humanos en las medidas adoptadas.

2. ¿Qué es el ciberterrorismo? Concepto y elementos.

Es habitual que el punto de partida de un trabajo sea la definición del fenómeno de estudio o, al menos, plantear cuáles son las distintas definiciones existentes para posicionarse a favor de alguna de ellas. No es extraño tampoco que, tras analizar detalladamente los defectos y virtudes de cada una de ellas, el autor crea conveniente adoptar una posición ecléctica y presente una definición propia con algunos elementos de las ya existentes. En el caso del ciberterrorismo iniciar un trabajo con este método, detallando cada una de las tesis existentes para después analizarlas, plantea una serie de problemas que escapan al objetivo del presente trabajo. El primer problema aparece con la propia definición de terrorismo sobre la que no existe ni siquiera acuerdo a nivel internacional, sino una amplia amalgama de propuestas[1] y una negociación indefinida en el seno de las Naciones Unidas[2]. El segundo, determinar qué actos de terrorismo pueden considerarse como cometidos en el ciberespacio.

Teniendo en cuenta las reflexiones anteriores, en este epígrafe vamos a presentar los principales conceptos acerca de la posible actuación terrorista en el ciberespacio, de forma muy general que permita al menos determinar qué instrumentos existentes

[1] Ya en un estudio de 1988 se identificaban 22 elementos distintos en 109 definiciones discutidas. *Vid.* SCHMID, A.P. y JONGMAN, A.G., *Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories and Literature*, Transaction Books, New Brunswick, 1988, p.5.

[2] Para un análisis de las propuestas en el seno de la Asamblea General de Naciones Unidas, *Vid*. SAMUEL, K.L.H., "The Rule of Law Framework and its Lacunae: Normative, Interpretative and/or Policy Created?", en SALINAS DE FRÍAS, A.M., SAMUEL K.L.H. y WHITE N.D., *Counter Terrorism: International Law and Practice,* Oxford University Press, New York, 2012, pp.16-21.

podrían aplicarse en la lucha contra esta amenaza en el espacio virtual. Para ello comenzaremos esbozando una definición genérica de terrorismo con el fin no de establecer un concepto inamovible sino de presentar una idea básica de las situaciones que encontramos al hablar de terrorismo. Tras ello, en un apartado posterior, trataremos cómo se reflejan los elementos propios de las actividades terroristas en el espacio cibernético.

Con vistas a aportar los elementos generales del terrorismo, y recordando la carencia de una definición ampliamente aceptada, acudiremos a los trabajos del primer tribunal internacional que se pronunció respecto a una definición general de este fenómeno en el derecho internacional. Nos referimos al Tribunal Especial para el Líbano (en adelante, STL por sus siglas en inglés). La Sala de Apelaciones de este Tribunal determinó que, si bien existían discusiones entre los expertos juristas a la hora de abordar este problema, una serie de elementos comunes habían comenzado a formar *opinio iuris* en la comunidad internacional, al menos en tiempo de paz.

Es por ello que los distintos instrumentos internacionales, las resoluciones de Naciones Unidas y las prácticas judiciales y legales de los Estados evidenciarían, a juicio del STL, el surgimiento de una norma de derecho consuetudinario respecto al crimen internacional del terrorismo. Los elementos claves identificados por este tribunal especial son los siguientes: la perpetración de un acto criminal (como asesinato, secuestro, toma de rehenes, incendios provocados y otros) o la amenaza de realizar tales actos (a); la intención de extender el miedo entre la población (lo que conlleva generalmente la creación de un peligro público) o directa o indirectamente coercer a una autoridad nacional o internacional para que realice alguna acción o deje de realizar alguna (b); y cuando el acto incluye elementos transnacionales (c).[3]

Aplicando los elementos genéricos anteriores, podría calificarse como ciberterrorismo la convergencia de esta clase de actos en el ciberespacio. Inicialmente,

[3] STL*, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, 16 de febrero de 2011, Case No. STL-11/01/I, párs. 83 a 85. Disponible online en: http://www.stl-tsl.org/en/rule-176bis-decision (Última visita el 29/06/2015)

la primera visión que puede acudir a quien se plantea este problema es la de un ataque terrorista a gran escala contra las estructuras de la sociedad de la información. No obstante, desde que hemos partido de una convergencia entre terrorismo y ciberespacio, no se puede reducir el campo de actuación a los ataques directos sino que se deben tener en cuenta aquellas otras formas de actuación de los grupos terroristas como son la propaganda y el reclutamiento a través de Internet. Es precisamente en este último aspecto, como ya se ha indicado, en el que centraremos nuestro trabajo desde el punto de vista de la seguridad.

Siguiendo con la línea anteriormente introducida, estas páginas se centran en aquellos usos terroristas del ciberespacio distintos a los ataques directos. ¿Por qué centrar el trabajo en este aspecto y no en la defensa? Por dos razones principales. La primera sugiere, dado que este trabajo se centra en la Unión Europea (en adelante, UE), que las competencias de esta organización en materias distintas a la política de defensa son mucho más amplias y permiten una mayor actuación, sin despreciar la importancia que tiene la defensa en este aspecto y la necesidad real de coordinar acciones con la Organización para el Tratado del Atlántico Norte. La segunda, que la mayoría de los grupos terroristas no suelen tener las habilidades tecnológicas necesarias para llevar a cabo con éxito ataques en este campo[4]. El principal atractivo que ofrece Internet no es un método de ataque sino una vía para agitar a la opinión pública, reclutar y educar miembros; controlar la organización, realizar propaganda e incluso instruir sobre cómo cometer atentados.

De este modo, y con el objetivo de determinar qué medidas existen y cuáles deberían existir a la hora de incrementar la seguridad en la UE contra los contenidos terroristas en Internet, este epígrafe se centrará en identificar los cuatro tipos básicos de contenido ilegal a combatir: la presentación de los puntos de vista de los terroristas; la diseminación de amenazas y propagandas; el reclutamiento y entrenamiento de miembros y, por último, las actividades de búsqueda de financiación.

[4] DOGRUL, M., ASLAN A. y CELIK E., "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", *3rd International Conference on Cyber Conflict,* Tallin, CCD COE Publications, 2011, p. 32.

2.1 Internet: una herramienta eficaz para la difusión de los ideales terroristas

El principal obstáculo al que se enfrenta un grupo terrorista a la hora de extender sus dictados, objetivos y ambiciones es evitar ser detectado por las fuerzas estatales de seguridad. Si bien es cierto que el uso de folletos[5] y del "boca a boca" son un medio de propaganda a tener en cuenta a la hora de reclutar miembros, también lo es que suponen un elevado riesgo para los emisores y que su rango de influencia es muy reducido[6].

El auge de Internet, con su fácil acceso y bajo coste, ha eliminado casi por completo esta traba que se presentaba a las organizaciones terroristas. El avance de las nuevas tecnologías, aunque proporciona grandes beneficios para la sociedad en general, también ha permitido que la mayoría de grupos terroristas mantengan sitios webs propios en los que se contienen, entre otros, datos sobre su historia y principales éxitos[7]. Los datos, recopilados y presentados para el público objetivo[8], son incluso traducidos en diferentes lenguas para que los ciudadanos extranjeros puedan comparar los puntos de vista terroristas con los ofrecidos por los medios de comunicación.

Teniendo en cuenta el objetivo propagandístico anterior, las páginas web patrocinadas por grupos terroristas para cometer atentados no suelen, por lo general, realizar un enaltecimiento injustificado de la violencia empleada. Al contrario, presentan su situación como la respuesta de la oposición política a ataques extranjeros contra su libertad de expresión para así poder atraer la empatía de los defensores occidentales de las libertades civiles. Y qué mejor medio para hacerlo que Internet, considerado máximo símbolo de la libertad de expresión sin censuras. En esta línea se

---

[5] Hay que resaltar en este punto las recientes iniciativas del Estado Islámico en el aspecto propagandístico. Este grupo, que cuenta con un gran territorio ocupado y sus fuentes de recursos, suma a las conquistas territoriales una revista propia ampliamente difundida, también en Internet. La revista "Dabiq", con informes y eventos del Estado Islámico, se centra especialmente en animar al reclutamiento de ciudadanos occidentales. El último número puede consultarse online en: http://media.clarionproject.org/files/islamic-state/isis-isil-islamic-state-magazine-issue+8-sharia-alone-will-rule-africa.pdf (Última visita el 29/06/2015)

[6] BRUNST, P.W., "Threat Analysis: Use of the Internet for Terrorist Purposes and Cyberterrorism", en SIEBER, U. y BRUNST, P.W., *Cyberterrorism and Other Use of the Internet for Terrorist Purposes: Threat Analysis and Evaluation of International Conventions,* Council of Europe Publishing, 2007, p. 33.

[7] Para un informe detallado sobre los usos terroristas más recientes en Internet *vid.* International Institute for Counter-Terrorism, "Cyber-Terrorism Activities", Report No. 11, October-December 2014, pp. 1-39.

[8] WEIMANN distingue tres audiencias diferentes: *supporters, international opinion* y *enemy publics. Vid.* WEIMANN. G., "How Modern Terrorism Uses the Internet", *United States Institute of Peace*, Special Report 116, Marzo de 2004, pp. 4 y 5.

han identificado tres estructuras comunes en estas webs a la hora de justificar esta violencia[9].

La primera de las estructuras mencionadas anteriormente consiste en presentar la violencia como única respuesta posible ante la opresión del enemigo, calificando las actuaciones estatales como "asesinatos" o "genocidios". La segunda, en maximizar la actuación del enemigo para legitimar así la violencia empleada por el grupo terrorista como un acto de defensa frente a una agresión, autodenominándose "luchadores de la libertad". Y, por último, emplear el lenguaje de la no violencia cuando confirman la búsqueda pacífica de soluciones y solicitan la presión internacional ante un gobierno represivo. La importancia de estos contenidos en plataformas virtuales no debe despreciarse, máxime teniendo en cuenta la situación actual de crecimiento del número de "combatientes extranjeros" incorporados al Estado Islámico[10].

2.2 Propaganda y amenaza terroristas a través de las nuevas tecnologías

El terrorismo ha sido calificado en no pocas ocasiones como una forma de guerra psicológica, y desde luego Internet es un frente idóneo para continuar con esta campaña. La diseminación de vídeos en los que se muestran actos terroristas quizás sea el más ejemplificativo y actual dada la práctica del Estado Islámico de colgar en Internet ejecuciones de rehenes, comenzando con la decapitación del periodista estadounidense James Foley. En el caso de Al Qaeda, los atentados del 11S contra el World Trade Center fueron seguidos por una continua campaña publicitaria en Internet cuyo mensaje principal era el próximo lanzamiento de ataques a gran escala contra el territorio estadounidense.

De igual modo, tras la intervención militar francesa en Mali se incrementó de forma exponencial el número de llamamientos en Internet a realizar atentados individuales junto con instrucciones para llevarlos a cabo[11].

---

[9] WEIMANN G., *Ibídem*, p. 6.

[10] Tras los atentados cometidos en París en enero de 2015 los ministros de Justicia e Interior de la UE, conscientes de esta realidad, solicitaron la cooperación de la industria de Internet en la lucha contra estos contenidos ilegales. El documento de la Declaración de Riga puede consultarse online en: https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf (Última visita el 29/06/2015)

[11] Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2014. Disponible online en: https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014 (Última visita el 29/06/2015)

La sensación de inseguridad que crean anuncios de tales características, ampliamente cubiertos por los medios de comunicación, son especialmente graves máxime tras la magnitud de un atentado como el cometido contra las Torres Gemelas. Las páginas web vinculadas a Al Qaeda incluso clamaban el golpe asestado a la seguridad de los inversiones en el mercado estadounidense[12]. Sensación a la que no fueron ajenos los países de la Unión Europea: Austria y Alemania, entre otros países, recibieron amenazas de Al Qaeda en vídeos colgados en Internet debido a implicación en Afganistán[13].

Las páginas web adolecen, pese las múltiples posibilidades de amenaza y propaganda expuestas, de una grave desventaja. El hándicap consiste en que sólo los realmente interesados en esta tipología de contenidos accederán a una información que comparte el ciberespacio con miles de millones de webs[14]. Es por ello que las organizaciones terroristas son cada vez más activas en la búsqueda y empleo de otros medios virtuales que les permitan presentar sus puntos de vista incluso a aquellos que no los buscan activamente. Nos referimos, por supuesto, a las plataformas sociales en las que crear una cuenta pública donde anunciar contenidos se beneficia de mayores facilidades incluso que la propia creación de páginas web. Los soportes informáticos ofrecidos por estas redes sociales permiten no sólo colgar vídeos de contenido violento acompañados de música moderna para atraer al público más joven, sino también programas de radio.

De este modo, los mismos medios (*YouTube, Facebook, Twitter*) que sirvieron para propagar los movimientos de la Primavera Árabe han sido también el cauce para extender el radicalismo islamista a través de todo el mundo. Es interesante en este punto destacar cómo contenidos elaborados por grupos situados en la Unión Europea y con este territorio como objetivo no alojan esta información en servidores europeos, lo cual

[12] Para un análisis del impacto económico de los ataques, ver Congressional Research Service, "The Economic Effects of 9/11: A retrospective Assesment", 2002.
Disponible online en: http://fas.org/irp/crs/RL31617.pdf (Última visita el 29/06/2015)
[13] El vídeo fue publicado en el sitio web "Global Islamic Mediafront". Para más información ver STEINBERG, G.W., *German Jihad. On the Internationalization of Islamist Terrorism,* Columbia University Press, New York, 2013, p. 135.
[14] Según "Internet Live Stats" la cifra rozó los mil millones en el año 2014. Datos disponibles online en: http://www.internetlivestats.com/total-number-of-websites/ (Última visita el 29/06/2015)

podría caer en el ámbito de aplicación de delitos como el de incitación a la violencia o discursos del odio[15].

El almacenamiento anterior se realiza en servidores localizados, por extraño que pueda parecer en principio, en los propios Estados Unidos. La razón recae en la Primera Enmienda a la Constitución de los Estados Unidos. Estas líneas, fuertemente respaldadas por el poder judicial estadounidense, proporcionan una amplia protección a la libertad de expresión de los proveedores de Internet que permiten la utilización de sus servidores para almacenar contenidos de grupos terroristas[16]. Nos encontramos de nuevo ante la dicotomía de encontrar el precario punto de equilibrio entre la seguridad y la protección de las libertades civiles.

2.3 Reclutamiento y entrenamiento de terroristas a través de la red: ¿una universidad abierta para la yihad?

El título de este epígrafe contiene dos de los elementos claves para la supervivencia de los grupos terroristas: el reclutamiento y entrenamiento de sus miembros. Antes de la generalización de Internet la búsqueda de determinados contenidos relacionados con atentados terroristas podía ser detectado de manera relativamente eficaz. Por ejemplo, el registro de libros de una biblioteca podía mostrar intereses en la fabricación de bombas[17]. O la asistencia a determinados lugares preestablecidos por las fuerzas de seguridad e inteligencia podía iniciar la sospecha del interés de un sujeto por afiliarse a una organización con objetivos terroristas, realidad muy presente en la Unión Europea y que sigue causando acaloradas discusiones entre los partidarios de un mayor peso de la seguridad y quienes defienden a ultranza el respeto a los datos personales[18].

---

[15] Ejemplo de ello son la sección 131 del Código Penal Alemán o, más cercano, el artículo 510 del Código Penal español.

[16] Para un análisis más profundo *vid.* KLAUSEN, J., BARBIERI E., REICHLIN-MELNICK A. y ZELIN Y.A., "The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun's Propaganda Campaign", *Perspectives on Terrorism*, vol. 6, nº1, 2012.
Disponible online en:
http://www.terrorismanalysts.com/pt/index.php/pot/article/view/klausen-et-al-youtube-jihadists/html
(Última visita el 29/06/2015)

[17] Para un resumen de la relación entre el control de las bibliotecas y la lucha contra el terrorismo en EEUU vid. GILBERT, E.D, "Confidentially Speaking: American Libraries and the USA PATRIOT Act", *Library Philosophy and Practice,* vol. 8, nº1, 2005.

[18] Un análisis detallado de cómo afecta la entrada en vigor del Tratado de Lisboa a los Acuerdos PNR puede encontrarse en QUESADA GÁMEZ, M. y MINCHEVA E., "No Data Without Protection? Re-

La aparición de Internet ha jugado, como en epígrafes anteriores, un papel protagonista en la nueva orientación de estos grupos a la hora de captar y entrenar miembros. La posibilidad de colgar contenidos en una plataforma fácilmente accesible y sujeta a pocas censuras ha conllevado la aparición de manuales electrónicos en los que se explica detalladamente cómo cometer actos terroristas[19]. Este fenómeno ha sido denominado por algunos autores como la creación de una "universidad abierta para la yihad"[20], impresión confirmada por la multiplicidad tanto de documentos con contenidos específicamente terroristas como aquellos más genéricos que permiten obtener los mismos resultados. Es por todo ello que un gran sector del mundo del análisis de seguridad ve un mayor peligro real en este "cyberplanning" que en la propia posibilidad de atentados conducidos por el ciberespacio[21].

No obstante, y como ya hemos mencionado, Internet no sólo facilita el acceso a la información necesaria para cometer atentados sino que también es una plataforma idónea para el reclutamiento. El contacto entre la organización terrorista y el potencial miembro puede producirse en dos direcciones opuestas. La primera, y menos común, es que sea el propio interesado quien demuestre en Internet su deseo de unirse a uno de estos grupos. Fue el caso de Ziyad Kahlil, un estudiante de ciencias tecnológicas en el Columbia College de Missouri quien, tras administrar distintas webs de apoyo a Hamas, fue contactado por el grupo Al Qaeda para convertirse en el suministrador en EEUU de medios electrónicos para comunicar las distintas células terroristas[22].

Si bien es cierto que las anteriores situaciones no son extrañas, la práctica más habitual consiste en que sean las propias organizaciones terroristas quienes contacten

---

Thinking Transatlantic Information Exchange for Law Enforcement Purposes After Lisbon", en CARDWELL, P.J., *EU External Relations Law and Policy in the Post-Lisbon Era*, T.M.C. Asser Press, The Hague, 2012, pp. 287-312.

[19] Algunos como el "Terrorist's Handbook" o el "Anarchist Cookbook" están disponibles online y traducidos al español. En ellos se detalla, entre otras actividades, cuáles son los lugares idóneos para comprar los productos necesarios para fabricar un artefacto explosivo.

[20] PAZ, R., "Suicide or Martydom: The Roots of Anger that Motivated this Volcano", en DRONZINA, T., *Contemporary Suicide Terrorism: Origins, Trends and Ways of Tackling It"*, IOS Press, Ámsterdam, 2012, p. 36.

[21] THOMAS, T.L., "Al Qaeda and the Internet: The Danger of Cyberplanning", *Parameters,* vol. 23, Issue 1, Spring 2003, pp. 112-123.

[22] *Vid*. U.S. House of Representatives, "Progress since 9/11: the effectiveness of the U.S. anti-terrorist financing efforts : hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services", One Hundred Eighth Congress, first session, March 11, 2003.

con los posibles interesados antes que esperar la solicitud de los candidatos. Los potenciales miembros son el objetivo de una amplia campaña de propaganda que defiende los ideales de cada grupo concreto, como se ha expuesto anteriormente, y les anima a formar parte de ello facilitándoles datos sobre cómo unirse a su causa. Esta movilización en casos como el Estado Islámico es de tal calibre que ha llegado, incluso, a compararse con la realizada a través de videojuegos y películas norteamericanas para animar a la población a unirse al ejército[23].

A lo anterior hay que añadir que este reclutamiento no busca únicamente sumar miembros que cometan actos violentos, sino que también se dan una serie de pautas de comportamientos no violentos que pueden ayudar a la causa del grupo terrorista. Ejemplo de ello es el gran número de páginas web alrededor del mundo que se solidarizaron y elevaron protestas contra la detención de Abdullah Ocalan, líder del grupo terrorista kurdo PPK[24]. Todos los casos expuestos hasta aquí demuestran el peso de los contenidos publicados en Internet a la hora de mantener el funcionamiento de los grupos terroristas en áreas tan diversas como la formación, el reclutamiento o la publicidad. A continuación trataremos otro uso de Internet no menos relevante: el uso de las páginas web y las redes sociales como instrumento para obtener financiación.

2.4 Financiación del terrorismo a través de plataformas virtuales

La búsqueda de financiación por parte de los grupos terroristas también ha encontrado su lugar en Internet. Al igual que las organizaciones no gubernamentales y las fundaciones benéficas utilizan foros, redes sociales y webs para captar fondos, también lo hacen estos grupos con unos objetivos muy distintos. Una vez identificadas las personas con afinidad por la causa perseguida por el grupo terrorista, y en función de los datos personales existentes de ellas en la red, se inicia el contacto para solicitar donaciones. Ello suele realizarse a través de correos colectivos, páginas web

[23]ROSE, S., "The Isis propaganda war: a hi-tech media jihad", The Guardian, 7 de octubre de 2014. Disponible online en: http://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war (Última visita el 29/06/2015)

[24] WEIMAN, G., *Using the Internet for Terrorism Recruitment and Mobilization*, IOS Press, The NATO Science for Peace and Security Programme, Ámsterdam, 2007, p. 54.

administradas por terroristas o incluso espacios virtuales de fundaciones benéficas legítimas[25].

No obstante, las donaciones directas o indirectas no son el único modo de apoyar financieramente a los grupos terroristas bajo el anonimato del ciberespacio. Es por ello que hasta ahora se han identificado cuatro prácticas[26]: la solicitud directa, el comercio electrónico, la explotación de las herramientas virtuales de pago y el mencionado uso de las fundaciones benéficas. Así a la solicitud directa ya mencionada, consistente en correos colectivos y anuncios electrónicos, se suma en segundo lugar el comercio electrónico de productos como vídeos, libros o CDs cuyos beneficios van a parar a los fondos de las organizaciones terroristas.

El uso de herramientas virtuales de pago incluye, entre otros actos, el fraude, el robo de identidad y la sustracción de tarjetas de crédito. Un ejemplo del uso de tales actos lo ofrece el caso de *Reino Unido c. Younis Tsouli*[27]. Los beneficios del uso de tarjetas de crédito ajenas eran canalizados a través de cuentas de pago online como Paypal, recorriendo cuentas situadas en varios países hasta llegar al fondo deseado. El dinero sustraído era empleado principalmente para administrar páginas web en la que se anunciaban vídeos de Al Qaeda y proveer de equipamiento para actividades terroristas. Se calcula que 1400 tarjetas de crédito fueron usadas para generar, aproximadamente, 1,6 millones de libras destinadas a la financiación de estos grupos[28].

En cuanto a la financiación de organizaciones aparentemente legítimas, como fundaciones benéficas, también puede encontrarse en ciertos casos una vinculación con grupos terroristas. No es extraño que una organización benéfica, bajo el control o influencia en la sombra de un grupo terrorista, solicite donaciones online a favor de

[25] El 16 de octubre de 2014 fue lanzada en las redes sociales una campaña para financiar a los muyahidines en Gaza. A principios de julio de ese mismo año también fueron publicados en Internet documentos señalando las donaciones "bitcoin" como el mejor método para contribuir financieramente al objetivo del Estado Islámico. *Vid.* International Institute for Counter-Terrorism, "Cyber-Terrorism Activities", Reports nº 10 y 11.
[26] United Nations Office on Drugs And Crime, *The use of Internet for Terrorist Purposes*, United Nations Office, Viena, 2012, p. 7.
[27] En el caso *R v. Tsouli and others*, Younes Tsouli, Wassem Mughal y Tariq al-Daour fueron declarados culpables de cargos bajo la *Terrorism Act* de 2000, por incitación al asesinato con motivos terroristas dado el establecimiento y mantenimiento de páginas web y foros en los que se incitaba a cometer actos terroristas. *Vid. R v. Tsouli [2007] EWA (Crim) 3300.*
[28] *Ídem.*

causas supuestamente humanitarias. De las benéficas que han sido descubiertas en esta tesitura podemos destacar la *Benevolence International Fundation*, la *Global Relief Foundation* o la *Mercy International*, todas ellas empleadas como tapadera para financiar atentados terroristas en Oriente Medio[29].

3. Los instrumentos jurídicos de la Unión Europea en la lucha contra el ciberterrorismo

La línea seguida hasta el momento por el presente trabajo sustenta las afirmaciones realizadas en la introducción inicial. El objetivo no es estudiar los aspectos militares o los discursos políticos sobre Internet en los Estados miembros. La meta es presentar el papel de la Unión Europea en la consecución del ciberespacio como un espacio de libertad, seguridad y justicia. Tomando en consideración que gran parte de la vida de los ciudadanos se realiza conectada a Internet, no nos encontramos ante un problema superfluo. El siguiente paso del trabajo, una vez presentados cuáles son los usos terroristas *de facto* en Internet, es ineludible: identificar y analizar los instrumentos en materia de seguridad civil que pueden ser empleados en esta batalla global, así como las propuestas de mejora al respecto.

Una de las principales vías para combatir el ciberterrorismo y aumentar la seguridad en Internet es armonizar leyes nacionales. Este método permitiría en principio reducir la impunidad y evitar desigualdades en la prevención y persecución según el Estado donde se produzca el acto. En este campo, la UE goza de un papel protagonista dado que entre sus competencias figura la de adoptar normas mínimas y armonizar leyes penales nacionales, si bien está sujeta a unas estrictas limitaciones[30]. A continuación, y

[29] CONWAY, M., "Terrorist Use of the Internet and Fighting Back", *Information and Security: An International Journal,* vol. 19, 2006, p. 13.

[30] El artículo 83 TFUE divide esta competencia en dos grupos: a) para infracciones de especial gravedad y dimensión transfronteriza que obligan a la persecución común, recogiendo una lista taxativa en la cual el terrorismo aparece en primer lugar y b) para casos en que resulte imprescindible con vistas a garantizar la ejecución eficaz de una política de la Unión objeto de medidas de armonización. Es necesario resaltar que la lista de materias recogidas en el apartado 1 de este artículo se trata de una lista cerrada si bien el Consejo, por unanimidad y previa aprobación del Parlamento Europeo, puede ampliar esta lista conforme a los criterios indicados. En cuanto al apartado 2, algún autor lo considera como una vía para otorgar protección penal unitaria a los valores europeos, a los bienes jurídicos comunes europeos reconocidos consensualmente. Ejemplos de ello serían las disposiciones contra manipulaciones fraudulentas de las cotizaciones en la Bolsa o la corrupción activa y pasiva en el tráfico económico. *Vid.* SIEBER, U., "El futuro del Derecho penal europeo – Una nueva concepción sobre los objetivos y modelos del sistema penal europeo", en ALBRECHT, H.J., SIEBER, U., SIMON J.M. y SCHWAR, F., *Criminalidad,*

sin ánimo de entrar en un análisis profundo de los elementos de derecho penal, repasaremos qué normas existentes pueden aplicarse al uso concreto del terrorismo en Internet que estamos tratando: la difusión de contenido ilegal.

3.1 Decisión Marco sobre lucha contra el terrorismo

La Decisión del Consejo[31]recoge una serie de actos considerados terroristas. Basándose en criterios objetivos, la lista contiene entre otros los ataques contra la vida de las personas, atentados contra la integridad física, secuestro o retención de rehenes, destrucción de ciertas infraestructuras; ataques mediante aviones, barcos u otros medios de transporte público; el uso de armas, la liberación de sustancias peligrosas… En cuanto a los criterios subjetivos, el artículo 1 de la Decisión exige que el ataque suponga un grave daño contra un país u organización internacional y busque uno de los siguientes resultados: intimidar gravemente a una población (a), obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o abstenerse de hacerlo (b) , o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional (c).

Las ventajas de esta aproximación uniforme en la lucha contra el terrorismo son muy variadas. Así, en cuanto a la amenaza de cometer un acto terrorista que ocupaba el primer apartado del epígrafe anterior, el artículo 1 (i) prohíbe de forma clara "amenazar con cometer alguno de los actos de la lista". Esta redacción obliga a sancionar el acto ya sea cometido por las vías tradicionales o por Internet.

A la previsión anterior se suma la recogida en el artículo 2 sobre "delitos relativos a grupos terroristas. Entre ellos se encuentra la "participación en las actividades de un grupo terrorista, incluido el suministro de información o medios materiales, o mediante cualquier forma de financiación de sus actividades, con conocimiento de que esa participación contribuirá a las actividades delictivas del grupo terrorista". Este genérico apartado permitiría en principio incluir como delitos de

---

evolución del Derecho penal y crítica al Derecho penal en la actualidad, Editores el Puerto, Buenos Aires, 2009, pp. 36 y 37.

[31] Decisión Marco 2002/475/JAI del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo, DO L 164/3, 22.06.2002.

terrorismo tanto el reclutamiento y entrenamiento de terroristas como el apoyo financiero a través las plataformas virtuales[32], aunque la Decisión no menciona expresamente ni estos actos ni el uso de Internet.

La falta de especificidad de la Decisión respecto a los actos cometidos por Internet que estamos tratando en el presente trabajo es, no obstante, suplida con posterioridad. Así, en una Decisión del Consejo[33] del año 2008 se modifica la anterior con unas novedades muy vinculadas al ámbito que nos encontramos tratando. El Considerando 4 de dicha Decisión resume de forma clara la realidad que hasta ahora hemos descrito: "Internet se utiliza para inspirar y movilizar a redes terroristas locales e individuos en Europa y también sirve de fuente de información sobre medios y métodos terroristas, funcionando por lo tanto como un «campo de entrenamiento virtual». Por ello, las actividades de provocación a la comisión de delitos de terrorismo, la captación y el adiestramiento de terroristas se han multiplicado con un coste y unos riesgos muy bajos".

En esta Decisión la UE demuestra ser consciente de las amenazas que estamos tratando, desde la propaganda hasta el reclutamiento. Es por ello que el artículo 3 recoge ya de forma explícita la "distribución o difusión, por cualquier medio, de mensajes destinados a la comisión de los delitos" mencionados en el artículo 1, así como la "captación de terroristas" y el "adiestramiento de terroristas"[34]. Nos encontramos ante otro avance jurídico en la definición de aquellos mínimos que los Estados miembros deben incorporar a sus legislaciones penales[35].

[32] SIEBER, U., "Legal and Policy Evaluation: International Co-operation Against Terrorist Use of the Internet", en SIEBER U. y BRUNST P.W., *op. cit*., p. 79.
[33] Decisión Marco2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que se modifica la Decisión 2002/475/JAI sobre la lucha contra el terrorismo, DO L 330/21, 9.12.2008.
[34] El contenido de esta modificación ha sido fuertemente criticado por ciertos sectores al considerarlo contrario al artículo 12 de la Convención Europea de Derechos Humanos. *Vid.* Informe del Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, sobre la propuesta de decisión marco del Consejo por la que se modifica la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo, exposición de Dick Marty, 15 de mayo de 2008.
[35] En el caso español el contenido de esta Decisión fue incorporado mediante la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE núm. 152, de 23 de junio de 2010, páginas 54811 a 54883.

3.2 La Directiva de Comercio Electrónico

En apartados interiores hemos identificado Internet como el mejor ejemplo de plataforma para la libertad de expresión sin censuras. La persecución de contenidos ilegales terroristas en Internet exige, por tanto, la búsqueda de un precario equilibrio entre la seguridad y el derecho a la libertad de expresión, fundamento esencial de cualquier sociedad democrática. La Unión Europea no es ajena a esta realidad aunque no existen hasta la fecha documentos específicos al respecto[36]. Un ejemplo lo podemos encontrar en una de las Propuestas de Resolución Común sobre las medidas en la lucha contra el terrorismo[37]:

> "Observa con inquietud el incremento del uso de Internet y las tecnologías de la comunicación por parte de organizaciones terroristas para comunicarse, planear atentados y difundir propaganda; pide a las empresas de Internet y de redes sociales que colaboren con los Gobiernos y las autoridades policiales a fin de combatir este problema, al mismo tiempo que **se garantiza en todo momento el respeto a los principios generales de libertad de expresión** derecho a la intimidad; destaca que las medidas que limitan, con fines de lucha contra el terrorismo, el uso y la difusión de datos en Internet deben ser necesarias y proporcionales"[38].

Las empresas de Internet, tal y como recoge esta declaración, juegan un papel especialmente importante en la erradicación de los contenidos terroristas en el ciberespacio. Por regla general los proveedores de servicios de Internet transmiten y almacenan, junto a cantidades ingentes de información legal, contenidos de esta índole sin conocer su compatibilidad con los ordenamientos de los países a los que se dirigen. Una de las medidas que pueden plantearse es exigir responsabilidad a los proveedores que alojen estos datos. La cuestión yace, en este caso, en determinar cuáles son las condiciones para que dicha responsabilidad pueda exigirse.

---

[36] En el seno del Consejo de Europa sí se han producido avances específicos al respecto. Entre otros, *vid.* Declaración del Comité de Ministros sobre la libertad de expresión y de información en los medios de comunicación en el contexto de la lucha contra el terrorismo, 2 de marzo de 2005. Recientemente destaca el artículo 3 de la Declaración Conjunta sobre la Libertad de Expresión y las Respuestas a las Situaciones de Conflicto, de 4 de mayo de 1015, en el que se solicita a los Estados abstenerse de aplicar de forma amplia la restricción relativa al terrorismo.

[37] Propuesta de Resolución Común del Parlamento Europeo sobre las medidas de lucha contra el terrorismo, RC-B8-0122/2015, 10.2.2015, pár. 19.

[38] La negrita es nuestra.

La Directiva de Comercio Electrónico[39] se muestra como una herramienta útil a la hora de enfrentarse a estos dilemas. La norma armonizadora, en su búsqueda de la libre circulación de información entre los Estados miembros en el seno del mercado interior, prohíbe en su artículo 3.2 a los Estados miembros "restringir la libertad de prestación de servicios de la sociedad de la información de otro Estado miembro por razones inherentes al ámbito coordinado". Únicamente puede ser excepcionada esta prohibición en los casos establecidos en los apartados 4 a 6 de este mismo artículo. Y es dentro de los casos relativos al orden público donde podría incardinarse la opción barajada: "la prevención, investigación, descubrimiento y procesamiento del delito".

Una vez establecidos los casos en los que son aceptables las restricciones a la libertad de expresión, la Directiva busca armonizar la responsabilidad de las personas físicas y jurídicas que prestan servicios en la sociedad de la información. Al respecto, el artículo 14 impide a los Estados establecer responsabilidades a los prestadores siempre que se cumpla alguna de las siguientes dos condiciones: que no tenga un conocimiento efectivo de que la actividad es ilícita o que, conociéndolo, haya actuado con prontitud para eliminar o bloquear ese contenido. A continuación, el artículo 15 establece la imposibilidad de que los Estados miembros exijan a los proveedores búsquedas activas de contenidos ilícitos en su red. Con esta redacción, y teniendo en cuenta la ingente cantidad de información que es manejada diariamente por estos proveedores, es difícil imaginar la situación en la que no se cumpla la primera de las dos eximentes recogidas en el artículo 14.

Siguiendo con la problemática anterior, una solución viable para aumentar la implicación de los proveedores consistiría en crear mecanismos que alertasen a la empresa de la ilegalidad de los contenidos que transmite y aloja. Aunque la Directiva no recoja una regulación al respecto, su Considerando 40 sí reconoce esta necesidad: "Lo dispuesto en la presente Directiva deberá constituir una base adecuada para elaborar mecanismos rápidos y fiables que permitan retirar información ilícita y hacer que sea imposible acceder a ella; convendría que estos mecanismos se elaborasen

[39] Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, DO L 178, 17.7.2000.

tomando como base acuerdos voluntarios negociados entre todas las partes implicadas y fomentados por los Estados miembros".

La Directiva marca un camino a seguir pero se abstiene de realizar armonización jurídica alguna, una actitud muy criticada por la doctrina[40]. La única referencia al respecto en su articulado vinculante la encontramos al final del texto. Así, el artículo 21 impone a la Comisión Europea la obligación de presentar informes con propuestas para establecer mecanismos de "detección y retirada" de contenidos ilegales en Internet, así como los posibles instrumentos para exigir responsabilidad. La Directiva, no obstante, no impide que los Estados miembros establezcan estos mecanismos de "detección y retirada". El límite ese espíritu de la Directiva de mantener un alto estándar de protección del derecho a la libertad de expresión. Pocos son los países que han aplicado estos mecanismos, en la mayoría de los casos para proteger los derechos de autor o para erradicar la pornografía infantil[41].

La posibilidad de que sean los propios internautas quienes notifiquen la existencia de contenidos ilegales, entre ellos los de contenido terrorista, parece haberse enfrentado a férreos obstáculos pese a la alta utilidad que aparenta presentar. Es el caso de los preceptivos Informes que debía presentar cada dos años la Comisión Europea sobre los avances al respecto pero que se han encontrado en suspenso desde el año 2003[42].No puede decirse, sin embargo, que esta propuesta haya sido abandonada. En este sentido la Comisión Europea presentó en el año 2012 la iniciativa "Notice and Action"[43]. En ella se hace hincapié en la necesidad de establecer un marco horizontal común para esta clase de procedimientos en la lucha contra los contenidos ilegales, respetando siempre los principios de seguridad jurídica, proporcionalidad y respeto de

[40] *Vid.* DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet,* Aranzadi, Pamplona, 2011, pp.255-257; JULIÀ-BARCELÓ, R., "On-line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks", *European Intellectual Property Review*, vol. 22, Issue 3, March 2000, pp. 111 y 112.

[41] Italia, Francia, Alemania, Lituania, Finlandia y Hungría son ejemplos de esta situación. El único país europeo que contiene una previsión respecto al terrorismo es Reino Unido con la "Terrorism Act" de 2006.

[42] Comisión Europea, Comunicación COM(2003) 702 final de 21 de noviembre de 2003: primer informe sobre la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el mercado interior (Directiva sobre el comercio electrónico), pp. 16-18.

[43] Comisión Europea, Comunicación COM(2011) 942 final/2 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Un marco coherente para aumentar la confianza en el mercado único digital del comercio electrónico y los servicios en línea, 6.2.2012.

los derechos fundamentales[44]. La propuesta fue seguida de un periodo de consulta pública cuyas respuestas aún no han sido publicadas por la Comisión Europea[45]. La consulta formulaba una serie de preguntas, en lo que nos interesa, sobre la posibilidad de extender estos procedimientos a toda clase de contenidos ilegales, entre los que podríamos recoger los terroristas[46].

El empleo de la "detección y retirada" no es en modo alguno ajeno a la realidad. Así el propio TJUE, en el ámbito de la protección de los derechos de autor, ha considerado la existencia de notificaciones sobre contenidos ilegales como una de las vías que puede llevar al juez nacional a considerar la responsabilidad del operador de Internet[47]. O, en la misma línea anterior, el Protocolo firmado en mayo de 2011 entre los propietarios de derechos de autor y los operadores de Internet recoge no sólo un procedimiento de "detección y retirada" sino también otras medidas activas y preventivas, así como acciones contra infracciones repetidas. [48]

Las acciones en este campo, no obstante, parecen haberse estancado desde el año 2012. En abril de 2013 la Comisión presentó su "E-commerce Action plan 2012-2015" en el cual no se hace referencia alguna a medidas específicas para desarrollar procedimientos de "detección y retirada". No faltan observadores que atribuyen esta inactividad a la presión ejercida por los lobbies afectados y la especial sensibilidad con que se debe manejar este asunto, especialmente a la luz de las pasadas elecciones al Parlamento Europeo[49]. La preocupación por esta realidad se ha dejado notar entre los miembros del Parlamento Europeo en una carta al entonces Comisario de Mercado Interior y Servicios, Michel Barnier. Sus líneas resumen de forma clara la necesidad de

[44] Ibídem, p. 13.
[45]Comisión Europea, "A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries", 4.06.2012-11.09.2012.
[46] Algunos autores han publicado las respuestas enviadas. *Vid.,* por ejemplo, el documento presentado por European Digital Rights. Disponible online en: https://edri.org/files/05786204828112491 2Submission_EDRi_NoticeAction.pdf (Última visita el 29/06/2015)
[47] TJUE, sentencia de 12 de julio de 2011*, L'Oreal c. EBay*, C-324/09, Rec. pág. I-06011, pár. 122.
[48] Memorandum of Understanding, 4 May 2011, Brussels. Disponible online en: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (Última visita el 29/06/2015)
[49]KUCZERAWY, A., "Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative", *Computer Law and Security Review,* vol. 31, Issue 1, February 2015, p. 55.

avances con todas las garantías democráticas en un ámbito que reviste de una gran importancia para la lucha contra el ciberterrorismo[50].

3.3 La Directiva sobre Conservación de Datos y Directiva sobre la Privacidad y las Comunicaciones Electrónicas

Las nuevas formas de participación del terrorismo en Internet exigen, además de su identificación armonizada y eliminación de la red, técnicas especiales de prevención y persecución acordes con el terreno en el que se cometen: el ciberespacio. Al igual que los criminales emplean las nuevas tecnologías para actuar en la red de forma anónima, también deben emplearse nuevos mecanismos a la hora de identificar al perpetrador. Para ello es de vital importancia la preservación y expedición de los registros sobre el tráfico de datos, su recolección y aseguramiento conforme a las reglas jurisdiccionales del Estado en que se encuentren. La búsqueda del origen del contenido ilegal en Internet pasa precisamente por el recorrido que han seguido esos datos en Internet.

La existencia de mecanismos específicos en el espacio cibernético es esencial para la conducción exitosa de las investigaciones contra esta forma de terrorismo. Si el sujeto que cuelga los contenidos terroristas en Internet no lo realiza directamente desde su ordenador sino que, como es habitual, emplea ordenadores de terceros previamente hackeados para ocultar su sistema, el problema no tiene una fácil solución. Colgar contenidos desde su país hacia otro país a través de ordenadores situados en numerosas jurisdicciones nacionales hace que sea casi imposible rastrear más allá del último sistema empleado. La clave para poder ampliar la búsqueda consiste precisamente en el volumen de datos que hayan almacenado o no, por un periodo más o menos largo, los proveedores de Internet[51].

[50] "We have been reached by disturbing news that the proposal for a directive on notice and take-down that was produced by your services may not make it to the Parliament. As elected members and representatives of the European public, this is of high concern to us. The political process will not gain legitimacy if publically elected representatives are not allowed to scrutinize and debate proposals of concern in a transparent and democratic manner". Carta abierta de un grupo de Eurodiputados al Comisario Europeo para el Mercado Interior y Servicios, Michael Barnier, 3.07.2013. Disponible online en:http ://ameliaandersdotter.eu/sites/default/files/letter_commissioner_barnier_notice_and_takedown.pdf (Última visita el 29/06/2015)

[51] SIEBER,U., *loc. cit*., p. 82.

En la UE, una de las medidas más controvertidas a la hora de perseguir las actividades terroristas y mejorar la coordinación y disponibilidad de información se refiere, precisamente, a la retención de datos. Y es que el propio Consejo Europeo reconocía ya hace varios años la retención de datos como una de las medidas prioritarias en la lucha contra el terrorismo[52]. Como resultado, la Directiva sobre Conservación de Datos[53] fue adoptada, una medida en la lucha contra el terrorismo sin precedentes que requería el almacenamiento de los datos de todos los ciudadanos europeos en vistas a la persecución de los delitos más graves como el ciberterrorismo[54].

Generalmente, las investigaciones que persiguen los contenidos terroristas en Internet no suceden de forma automática sino que comienzan un tiempo después y necesitan, además, de un cierto tráfico de datos almacenado. Por ello, la Directiva establecía en su artículo 6 un periodo de conservación que obligaba a los Estados miembros a adoptar medidas para que cierto tráfico de datos fuese retenido por periodos no inferiores a seis meses y no superiores a dos años desde la fecha de la comunicación. Ello incluía, entre otros, los datos con respecto al acceso a Internet, el correo electrónico y la telefonía por Internet. Dicha retención era, sin duda, de especial utilidad para la investigación de las actividades terroristas en la red siempre y cuando se reduzca al máximo el impacto en el derecho a la protección de datos de los usuarios de Internet[55].

Como quizás se haya observado, hasta el momento hemos empleado el tiempo pasado para referirnos al contenido de la Directiva. La razón radica en una importante y reciente sentencia del TJUE[56] que declara inválida este acto legislativo. A continuación, expondremos de forma breve cuáles han sido los motivos recogidos en el pronunciamiento del TJUE que justifican eliminar del ordenamiento jurídico esta

[52]Declaración del Consejo Europeo sobre la lucha contra el terrorismo, 29.03.2004. Disponible online en: http://data.consilium.europa.eu/doc/document/ST-7906-2004-INIT/es/pdf (Última visita el 29/06/2015)
[53] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DO L 105, 13.4.2006.
[54] MARIE-HELEN, M., "The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?", *European Journal of Law and Economics*, nº33, 2012, p. 448.
[55] SIEBER, U., *loc. cit.,* p. 83.
[56] TJUE, sentencia de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros*, asuntos acumulados C-293/12 y C-594/12, no publicado aún en la Recopilación.

Directiva. Gracias a ello podremos, en etapa posterior, examinar las propuestas para reparar la situación con el máximo respeto al contenido de la sentencia.

El razonamiento parte de la base de que la conservación de los datos (que pueden aportar detalles muy precisos de la vida privada de una persona) y el acceso a ellos por las autoridades competentes supone una injerencia grave en los derechos fundamentales, al respeto a la vida privada y a la protección de datos de carácter personal. Pero tal injerencia puede resultar, como no es extraño en los ámbitos que afectan a la seguridad, justificada por determinados motivos que el TJUE pasa a considerar. Así, la conservación de estos datos y su transmisión responde a un objetivo de interés general como es la lucha contra la delincuencia grave y, con ello, la seguridad pública[57].

No obstante, y aunque el objetivo pueda justificar la medida, el TJUE encuentra fallos en el respeto al principio de proporcionalidad. La razón subyace, a juicio del TJUE, en una falta de regulación que garantice que las injerencias en los derechos fundamentales son las estrictamente necesarias. En concreto, la Directiva no realiza diferenciaciones, limitaciones ni excepciones a las personas, medios de comunicación y datos conforme al objetivo específico de lucha contra los delitos graves. Tampoco establece criterios objetivos que garanticen un acceso de las autoridades justificado por la gravedad del delito, sino que se remite de forma genérica a los "delitos graves" de cada ordenamiento interno. De igual modo hay una ausencia total de condiciones materiales y procesales que controlen el acceso y utilización de dichos datos[58].

En cuanto al periodo de conservación anteriormente mencionado, se repite el fallo de la generalidad al no establecer categorías en función de la categorías de los datos o del objetivo buscado. El periodo además oscila entre 6 y 24 meses sin que se realice indicación alguna de qué criterios deben regir un periodo más amplio o más reducido. A ello se suma la falta de garantías respecto a que los proveedores dispongan de los recursos necesarios para conservar los datos de forma segura, así como su destrucción definitiva transcurrido el periodo prescriptivo. Todo ello culminado por el hecho de que la Directiva no obliga a la conservación de los datos dentro del territorio

[57] *Ibídem*, pár. 41.
[58] *Ibídem*, pár. 64.

de la UE y, por tanto, no quedando sujetos al control de una autoridad independiente tal y como exige el artículo 8 de la Carta de Derechos Fundamentales de la UE[59] (en adelante, CDFUE)[60].

Todo lo anterior lleva al TJUE a declarar la nulidad de la Directiva sobre Conservación de Datos lo que, con efectos *ex tunc*, significa que debe reponerse la realidad existente anterior a la entrada en vigor de la Directiva. Tras esto, la única opción que en la UE permite a los Estados miembros retener datos se encuentra en la Directiva sobre la privacidad y las comunicaciones electrónicas[61]. En efecto, su artículo 15 permite tomar medidas restrictivas de la confidencialidad de las comunicaciones cuando "constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos". Para poder determinar la proporcionalidad de estas medidas se acudirá a la jurisprudencia conexa y la aplicabilidad de la CDFUE[62].

La desaparición de la Directiva sobre Conservación de Datos supone que ciertas formas de retención de datos puedan quedar desamparadas. El ámbito de aplicación de la Directiva de 2002 incluye a los proveedores de servicios de telecomunicaciones pero no a las redes sociales, las páginas web o los motores de búsqueda. La única posibilidad es la que ofrece el artículo 13 de la Directiva de Protección de Datos[63], al permitir limitaciones a los derechos y obligaciones en ella contenidas por una serie de razones concretas[64].

---

[59] *Ibídem*, pár. 68.
[60] Carta de Derechos Fundamentales de la Unión Europea, DO C 83/02, 30.3.2010, pp. 389 a 403.
[61] 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 (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201, 31.7.2002.
[62] STOEVA. E., "The Data Retention Directive and the right to privacy", *Academy of European Law Forum*, vol. 15, Issue 4, December 2014, p. 589.
[63] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281, 23.11.95.
[64] La seguridad del Estado; la defensa; la seguridad pública; la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en lasprofesiones reglamentadas; un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); la protección del interesado o de los derechos y libertades de otras personas.

En todas estas situaciones, tal y como se ha introducido anteriormente, los Estados están sujetos al cumplimiento estricto de los derechos fundamentales: "en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, incumbe a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también procurar no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho de la Unión, como el principio de proporcionalidad"[65]. Dicha salvaguardia de los derechos humanos en la protección de datos personales queda también claramente reflejada en la acción exterior de la UE[66].

Tomando en consideración todo lo anterior, ¿cómo es posible que la Unión Europea adopte una Directiva sobre Conservación de Datos? En otras palabras, ¿cómo puede ser la Directiva, de alguna forma, reparada? Antes de responder a estas preguntas hay que tener en cuenta que la retención de datos es una vía considerada aceptable por el TJUE a la hora de combatir el terrorismo, siempre y cuando se respeten los dictados de la Carta. El TJUE ofrece, de forma inusual, una serie de pautas a seguir por el legislador europeo y, a la postre nacional, a la hora de adoptar medidas en este ámbito concienciadas con la seguridad a la vez que respetan los derechos fundamentales[67].

Siguiendo con lo anterior, el primer aspecto a tener en cuenta es que la Directiva debe estar de algún modo orientada a las comunicaciones que guarden algún vínculo o relación con los delitos graves y el terrorismo. En términos más simples, el almacenamiento masivo de datos constituye una violación flagrante de la Carta conforme a los dictados del TJUE. En segundo lugar, la potencial Directiva debe

[65] TJUE, sentencia de 19 de abril de 2012, *Bonnier Audio y otros contra Perfect Communication Sweden AB*, C-461/10, ECLI:EU:C:2012:219, pár. 56.

[66] Recordemos que el Parlamento Europeo consiguió anular los Acuerdos PNR con Estados Unidos, siendo el necesario respeto de los derechos fundamentales uno de los caballos de batalla esgrimidos en su oposición. *Vid.* TJCE, sentencia de 30 de mayo de 2006, *Parlamento Europeo c. Comisión y Consejo*, asuntos acumulados C-317/04 Y C-318/04, Rec. Pág. I-0472. Para una visión de las relaciones de la UE con Estados Unidos *vid.* LIRORA DELGADO, I.: "Terrorismo y cooperación penal: ¿un contexto más favorable para los derechos humanos en las relaciones transatlánticas?", en *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, Servicio Editorial de la Universidad del País Vasco, Bilbao, 2010, pp. 363-394.

[67] PEERS S., "The data retention judgment: the CJEU prohibits mass surveillance", *EU Law Analysis*, 8 de abril de 2014. Disponible online en: http://eulawanalysis.blogspot.com.es/2014/04/the-data-retention-judgment-cjeu.html (Última visita el 29/06/2015).

subsanar los defectos de procedimiento señalados. Así, debería definir qué se entiende por "delitos graves"; establecer criterios objetivos a la hora de permitir el acceso a los datos; limitar el número de personas que puedan consultarlos, así como establecer una autoridad administrativa independiente que controle dichos accesos.

Junto a la anterior, se propone que la Directiva incluya reglas estrictas relativas al periodo de conservación, teniendo en cuenta las distintas categorías de datos, así como garantizar su protección frente a accesos y usos ilegales[68]. Deben indicarse además normas para destruir de forma efectiva los datos, que sólo puedan ser almacenados en el territorio de la UE y por tanto bajo el ámbito de aplicación de la CDFUE y las autoridades que la aplican. Estas son las posibles putas que podría seguir la potencial regulación al respecto. El nuevo paquete legislativo de protección de datos de la UE contiene un nuevo arsenal de medidas para proteger la privacidad de los ciudadanos europeos frente a los accesos de las agencias de seguridad. No obstante, los debates entre quienes se inclinan por una mayor protección de las libertades civiles y los defensores de la seguridad están retrasando la adopción de nuevas medidas hasta, al menos, el próximo año[69].

3.4 La Directiva sobre Prevención de Blanqueo de Capitales y Financiación del Terrorismo

La primera parte de nuestro trabajo consistía en una descripción de los principales usos que dan los grupos terroristas a Internet, siendo la búsqueda de financiación el último de ellos. La importancia de Internet como herramienta para obtener fondos no ha pasado desapercibida en las instituciones europeas. El ejemplo más reciente ello lo encontramos en el acto publicado el pasado día 5 de junio, una nueva Directiva sobre Prevención de Blanqueo de Capitales y Financiación del Terrorismo[70]. La juventud de esta norma provoca que los comentarios doctrinales al

[68] *Ídem.*
[69] FLEMING, J., "EU lawmaker warns of data protection rules delay till 2016", *EurActiv.com*, 14 de enero de 2015. Disponible online en http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100 (Última visita el 29/06/2015).
[70] Directiva 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, DO L 141, 5.06.2015.

respecto sean escasos, de forma que nos limitaremos a exponer las principales medidas que recoge esta norma en cuanto a la lucha contra la financiación del terrorismo en Internet.

Siguiendo a los atentados de París, Copenhague y Bruselas, el Consejo y la Comisión acordaron tomar nuevas acciones en la lucha contra la financiación del terrorismo. Para aumentar la eficacia de esas nuevas normas, ambas instituciones han realizado llamamientos para una implementación rápida y eficaz en los ordenamientos nacionales. Junto a ello, se solicita el fortalecimiento de la cooperación entre las Unidades de Inteligencia Financiera de los Estados miembros, así como medidas para una adecuada evaluación de riesgos con el asesoramiento de la UE. Estos son algunos de los puntos clave recogidos en la reciente Estrategia Europea de Seguridad Interior que será comentada en un epígrafe posterior.

El nuevo marco reforzado de lucha contra la financiación del terrorismo establece tres vías de acción principales: facilitar el trabajo de las Unidades de Inteligencia Financiera de los diferentes Estados miembros a la hora de identificar y perseguir transferencias sospechosas y facilitar el intercambio de información (a); establecer una política coherente con los países no miembros de la UE que tienen regímenes deficientes de lucha contra la financiación del terrorismo (b); y asegurar un completo seguimiento de las transferencias de fondos desde y hacia la Unión Europea.[71]

Hay que mencionar, en lo que a nuestro trabajo nos interesa, que todas las previsiones recogidas en esta nueva Directiva son completamente aplicables a las actividades realizadas en Internet. Así lo recoge expresamente en su Considerando 18: "La presente Directiva debe aplicarse igualmente a aquellas actividades de las entidades obligadas a las que es aplicable la presente Directiva que se lleven a cabo a través de internet".

La medida concreta que se encuentra quizás más conectada con el itinerario seguido hasta ahora por nuestro trabajo es la relativa al registro centralizado de datos. Por vez primera, tal y como recoge el Considerando 14, los Estados miembros están

[71]Comisión Europea, "European Parliament backs stronger rules to combat money laundering and terrorism financing", *Press Release*, 20 May 2015.

obligados a mantener registros centralizados de datos sobre los beneficiarios últimos de las transacciones financieras. Los registros no son, evidentemente, públicos sino que son únicamente accesibles por las autoridades competentes y las Unidades de Inteligencia Financiera. También se permite el acceso a personas con un interés legítimo, como investigadores y otros ciudadanos afectados.

El amplio conjunto de medidas para acceder a estos datos y los objetivos de su uso parecen seguir las pautas ya indicadas en el epígrafe anterior establecidas por el TJUE[72]. Así parece entenderse en otras instancias internacionales como Naciones Unidas, reconociendo al proyecto un ánimo de transparencia y de lucha contra la delincuencia[73]. Ello supone, por tanto, una posibilidad de conservación información, al menos en el sector financiero, respetuosa con las exigencias de la protección de datos[74].La aprobación de la nueva Directiva parece por ahora un paso más contra los usos terroristas de Internet, tal y como manifestó la Comisaria de Justicia, Věra Jourová, al conocer su aprobación por el Parlamento Europeo[75].

4. La relación entre Internet y Terrorismo en las Estrategias y Agendas de la Unión Europea

Junto a los instrumentos jurídicos anteriormente mencionados, la Unión Europea también ha elaborado una serie de documentos políticos no menos importantes denominados "estrategias" y "agendas". No puede finalizarse este trabajo sin hacer mención a este método con que la Unión Europea establece los objetivos y líneas de actuación a la hora de luchar contra la amenaza terrorista e incrementar la seguridad en Internet. Y en este punto de enfrentarse a los retos cibernéticos la UE no se ha quedado

[72] *Vid. supra* p. 22.
[73] Consejo de Derechos Humanos de Naciones Unidas, "Illicit financial flows, human rights and the post-2015 development agenda", A/HRC/28/60, 10 de febrero de 2015, p. 19. Disponible online en: http://www.ohchr.org/Documents/Issues/Development/IEDebt/A_HRC_28_60_en.pdf (Última visita el 29/06/2015).
[74] Normativa que se encuentra actualmente en proceso de actualización y se prevé su acuerdo para finales de 2015. *Vid.* Comisión Europea, "Apoyo de los ministros de Justicia a la propuesta de la Comisión de fijar nuevas normas de protección de datos para impulsar el mercado único digital de la UE", Comunicado de Prensa, 15 de junio de 2015. Disponible online en: http://europa.eu/rapid/press-release_IP-15-5176_es.htm (Última visita el 29/06/2015).
[75] "Serious and organised crime is driven by profit - tracing the illicit proceeds of crime back to the criminal networks is essential both to detect, prosecute and dismantle those networks and to seize and confiscate their criminal wealth. The new anti-money laundering rules adopted today will help us follow the money and crack down on money laundering and terrorist financing Comisión Europea, "European Parliament…", *Ídem*.

corta en Estrategias. De la gran variedad de documentos no jurídicos relativos al ciberespacio y el terrorismo, las estrategias más destacadas se refieren a la lucha contra el terrorismo, la ciberseguridad y la seguridad interior[76].

Ya en el año 2005 la Unión Europea era consciente de las amenazas que suponían los contenidos terroristas en Internet. En su Estrategia sobre lucha contra el terrorismo[77] se hacen varias referencias explícitas que posteriormente se han traducido, en mayor o menor medida, en los actos legislativos que ya hemos examinado. Así, encontramos en su apartado 9 que deben limitarse las actividades que "tengan un papel en la radicalización, evitando el acceso a la formación terrorista, estableciendo un marco jurídico sólido para prevenir la captación, y estudiando maneras de impedir la captación de terroristas a través de Internet".

El apartado 28 no es menos taxativo al respecto cuando afirma que" debería impedirse su capacidad de comunicación [de los terroristas] y planificación pasase inadvertida, mediante medidas como la retención de datos de telecomunicación. Deberían también eliminarse, hasta donde sea posible, las oportunidades que ofrece Internet para comunicase y diseminar la experiencia técnica relacionada con el terrorismo". A ello se suma, en el marco de la cooperación judicial, el establecimiento de un marco legal para la eliminación de los contenidos terroristas presentes en la red.

Y es en ese mismo año, con la consciencia de la UE de la especial atención que merece atajar la radicalización y captación de terroristas, cuando la UE presenta una específica Estrategia para luchar contra la radicalización y la captación de terroristas[78], revisada por última vez en 2007[79]. Así se habla en su apartado 9 de la necesidad de

[76] No trataremos la famosa Estrategia Europea de Seguridad[76] ya que, aunque contiene alusiones a la importancia de la lucha contra el terrorismo, son medidas desarrolladas en las Estrategias posteriores y apenas mencionan el elemento cibernético más allá de la conexión por "redes electrónicas".

[77] Consejo de la Unión Europea, "Estrategia de Lucha contra el Terrorismo", 14469/3/05, 30 de noviembre de 2005.
Disponible online en: http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=es (Última visita el 29/06/2015).

[78] Consejo de la Unión Europea, "Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas", 14781/1/05, 24 de noviembre de 2005.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-14781-2005-REV-1/es/pdf (Última visita el 29/06/2015).

[79] Consejo de la Unión Europea, "Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas – Informe de su aplicación", 15443/07, 23 de noviembre de 2007.

"establecer un marco jurídico apropiado para impedir la incitación a la violencia y su legitimación y estudiaremos medios para impedir la captación de terroristas a través de internet". En la revisión se acentúa aún más la importancia de la actuación en el ciberespacio, referenciando iniciativas específicas de lucha contra los contenidos terroristas en Internet. Así se menciona el mecanismo "Check the Web" destinado a reforzar la cooperación en materia de control y análisis de los sitios de Internet. Este programa cuenta con el respaldo específico de la UE y permitió la apertura de un portal informativo en Europol donde conectar a expertos que se encargan de la evaluación del uso de internet por los grupos terroristas[80].

En cuanto a la Estrategia de Ciberseguridad[81], no son demasiadas las referencias realizadas al terrorismo. No obstante, las pocas líneas de referencia encierran un gran contenido y potencial. La primera línea de actuación se refiere al apoyo que prestará la Comisión Europea a las investigaciones que en el marco de la Estrategia 2020 estén destinadas a reducir la actividad terrorista en el ciberespacio. La segunda tiene un importante impacto en la acción exterior de la UE al subrayar el apoyo "junto con los socios y organizaciones internacionales clave, el sector privado y la sociedad civil, el desarrollo de capacidades globales en los terceros países para mejorar el acceso a la información y a una Internet abierta, prevenir y combatir las ciberamenazas, incluidos los incidentes accidentales, la ciberdelincuencia y el ciberterrorismo, e impulsar la coordinación entre los donantes para orientar los esfuerzos de desarrollo de capacidades"[82].

La última que comentaremos es la Estrategia de Seguridad Interior[83]. Su objetivo segundo, referente a la prevención del terrorismo, recoge de forma clara la importancia del tema objeto del presente trabajo: "Actualmente, las amenazas proceden

---

Disponible online en: http://data.consilium.europa.eu/doc/document/ST-15443-2007-INIT/es/pdf (Última visita el 29/06/2015).

[80] Consejo de la Unión Europea, "Conclusiones del Consejo sobre la cooperación en la lucha contra la utilización de Internet por terroristas (Check the web)", 8457/07, 19 de abril de 2007.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-8457-2007-INIT/es/pdf (Última visita el 29/06/2015).

[81] Comisión Europea, Comunicación Conjunta JOIN (2013) 1 final al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de ciberseguridad de la Unión Europea: un espacio abierto, protegido y seguro, 7 de febrero de 2013.

[82] *Ibídem*, p. 18.

[83] Comisión Europea, Comunicación COM (2010) 673 final al Parlamento Europeo y al Consejo, la Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura, 22 de noviembre de 2010.

tanto de las organizaciones terroristas como de los denominados «lobos solitarios», que han podido desarrollar sus creencias radicales a partir de la propaganda extremista y encuentran material de formación en Internet. Nuestros esfuerzos para combatir el terrorismo deben centrarse en adelantarnos a la amenaza con un enfoque europeo coherente que incluya la acción preventiva". Asimismo se promueve la creación de una "red de la UE para la sensibilización frente a la radicalización" en la que la Comisión apoyará los trabajos de la sociedad civil destinados a luchar contra la propaganda extremista violenta en Internet.

En cuanto al objetivo tercero, relativo al aumento de la seguridad de los ciudadanos y empresas en el ciberespacio, una de las acciones contempladas se refiere a los contenidos terroristas en Internet. La Estrategia dice aquí que "el tratamiento de los contenidos ilegales de Internet incluida la incitación al terrorismo debería ser conforme a las directrices sobre cooperación, basadas en procedimientos autorizados de detección y retirada". Las consecuencias jurídicas de estas propuestas ya han sido analizadas con anterioridad por lo que no es necesario profundizar en más en ellas[84].

Respecto a a las Agendas, la que aquí nos interesa es la Agenda Europea de Seguridad[85]. De reciente publicación, contiene una batería de propuestas de repercusiones nada desdeñables en la lucha contra el terrorismo en Internet. Identificando el terrorismo y la ciberdelincuencia como dos de las prioridades esenciales de la Agenda para una acción inmediata, las principales acciones que presenta son: reforzar las acciones de apoyo de Europol, reuniendo las capacidades policiales de lucha contra el terrorismo en un Centro Europeo de Lucha contra el Terrorismo en el seno de Europol (a); poner en marcha el foro de la UE con empresas del sector de las TI para desarrollar herramientas de lucha contra la propaganda terrorista y abordar preocupaciones con respecto a las nuevas tecnologías de cifrado (b); abordar nuevas medidas para la lucha contra la financiación del terrorismo (c); abordar las posibles lagunas en la lucha contra la incitación al odio en Internet (d); y revisar la Decisión Marco sobre el terrorismo con una propuesta en 2016 (e).

[84] *Vid. supra* p. 18.

[85] Comisión Europea, Comunicación COM (2015) 185 final final al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Agenda Europea de Seguridad, 28 de abril de 2015. Disponible online en: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-185-ES-F1-1.PDF (Última visita el 29/06/2015).

La importancia de todos estos instrumentos políticos radica en su papel de "preludio" de lo que será o bien la actualización de los instrumentos jurídicos actuales o bien la creación de otros nuevos. Como hemos podido observar, gran parte del contenido de estos documentos se refiere a la mejora de los sistemas ya recogidos en Directivas o Decisiones, así como plantear la creación de otros nuevos con un punto de vista modificado según el avance de las amenazas y de la propia realidad jurídica (la anulación de un acto legislativo es una claro ejemplo de ello). Y son estos contenidos políticos y jurídicos los que nos permiten elaborar una serie de conclusiones en el siguiente y último apartado.

5. Conclusiones

El comienzo del presente trabajo reflejaba que el principal uso de Internet por los terroristas consiste en la diseminación de contenidos ilegales. Este nuevo medio de comunicación es empleado de forma abusiva por los terroristas a la hora de amenazar, incitar y publicitar el terrorismo; así como para el reclutamiento, entrenamiento y la financiación. Internet se ha convertido así en un importante activo a la hora de presentar sus mensajes frente al público de todo el mundo.

La exposición realizada hasta este punto nos ha permitido entrever cuáles son las luces y sombras en la respuesta de la UE ante la amenaza del ciberterrorismo. El número de instrumentos jurídicos producidos hasta la fecha no es nada desdeñable, teniendo siempre en cuenta que su impulso no comenzó verdaderamente hasta los ataques de Nueva York y Madrid. Y guardando, además, que los mayores avances se han visto en los últimos meses tras los brutales atentados sucedidos en París, Copenhague y Bruselas. Un ejemplo más, tristemente, de cómo la política antiterrorista avanza a golpe de atentado. El ordenamiento jurídico comunitario presenta pues una ventaja muy apreciable: ofrece a los Estados miembros un catálogo común de actividades consideradas terroristas. Esta realidad no es baladí si trasladamos la lucha contra una amenaza global y transnacional a un espacio donde estas características se maximizan: Internet. La definición de infracciones y métodos con un cierto nivel de consenso a nivel supranacional permite trasladar la prevención y persecución del terrorismo del nivel tradicional al existente, como hemos defendido, al ciberespacio.

No obstante, y pese a que los instrumentos y propuestas cubren gran parte de la realidad terrorista en Internet, no debe cejarse en los esfuerzos. El uso habitual de Internet con propósitos terroristas exige desarrollar más medidas que respalden necesidades reales de seguridad a la vez que respalden las libertades civiles. La prevención de contenidos ilegales no exige únicamente la armonización de normas penales sino también de los proveedores de Internet, que es la base del ya expuesto mecanismo de "detección y retirada" de la Directiva de Comercio Electrónico.

Tampoco podemos olvidar la imperiosa necesidad de la cooperación a la hora de perseguir los contenidos ilegales en la red. Para ello, los mecanismos de control y bloqueo de datos, como los recogidos en la caída Directiva sobre Conservación de Datos, son elementos de los que no se puede prescindir. No obstante, tal y como se ha encargado de recordarnos el TJUE, la sociedad democrática no puede dejar el internet bajo el libre albedrío de los usos terroristas pero tampoco puede establecer métodos de control inefectivos o simbólicos que dañen seriamente los derechos de información y protección de datos personales. En la búsqueda de esa "security-liberty frontier"[86], de ese óptimo de Pareto en términos económicos entre libertad y seguridad, las directrices de la jurisprudencia comunitaria pueden ser una buena base para encontrar el equilibrio entre las reclamaciones de "la libertad no tiene precio" y "seguridad a toda costa".

En este sentido, las iniciativas recogidas en las Agendas y Estrategias son también de gran ayuda. Entre ellas, una mayor implicación de los agentes sociales, de la sociedad civil y de los proveedores de Internet, trabajando codo con codo en la lucha contra los contenidos ilegales en Internet, es sin duda alguna una de las mejores vías a seguir. Internet, patrimonio común de la humanidad, se resiste por su propia naturaleza a ser controlado exclusivamente por los poderes públicos. Esto supone que la responsabilidad en la eliminación de los contenidos terroristas corresponda también a nosotros, la sociedad civil, principales usuarios del ciberespacio. Responsabilidad compartida, no obstante, que necesita de unos mecanismos efectivos y rápidos que conecten a los ciudadanos con los agentes con poder para eliminar contenidos y declararlos ilegales.

[86] POSNER E.A y VERMEULE A., *Terror in the Balance: Security, Liberty, and the Courts*, Oxford University Press, New York, 2007, p. 26.

La Unión Europea, como organización de perspectiva integradora, es la mejor herramienta a nuestro alcance para conseguir esa responsabilidad compartida a nivel europeo. La necesidad no es ya sólo conectar a los Estados en la lucha contra el ciberterrorismo, sino también a los propios ciudadanos europeos para que sean conscientes de la amenaza a la que se enfrentan y contribuyan a su erradicación. La importancia de la implicación de la ciudadanía en el proyecto europeo ya era proclamada por Jean Monnet. En su discurso del 30 de abril de 1952 ante la ciudad de Washington, este padre fundador de la UE pronunció una célebre frase que ilustra nuestra idea: "Nous ne coalisons pas des Etats, nous unissons des hommes".

6. Bibliografía

Monografías, artículos en revistas y obras colectivas

ALBRECHT, H.J., SIEBER, U., SIMON J.M. y SCHWAR, F., *Criminalidad, evolución del Derecho penal y crítica al Derecho penal en la actualidad,* Editores el Puerto, Buenos Aires, 2009

CONWAY, M., "Terrorist Use of the Internet and Fighting Back", *Information and Security: An International Journal,* vol. 19, 2006, p.p. 9-30.

DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet,* Aranzadi, Pamplona, 2011.

DOGRUL, M., ASLAN A. y CELIK E., "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", *3rd International Conference on Cyber Conflict,* Tallin, CCD COE Publications, 2011.

DRONZINA, T. (ed.), *Contemporary Suicide Terrorism: Origins, Trends and Ways of Tackling It"*, IOS Press, Amsterdam, 2012.

GILBERT, E.D, "Confidentially Speaking: American Libraries and the USA PATRIOT Act", *Library Philosophy and Practice,* vol. 8, nº1, 2005.

JULIÀ-BARCELÓ, R., "On-line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks", *European Intellectual Property Review*, vol. 22, Issue 3, March 2000.

KLAUSEN, J., BARBIERI E., REICHLIN-MELNICK A. y ZELIN Y.A., "The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun's Propaganda Campaign", *Perspectives on Terrorism*, vol. 6, nº1, 2012.

KUCZERAWY, A., "Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative", *Computer Law and Security Review,* vol. 31, Issue 1, February 2015.

MARIE-HELEN, M., "The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?", *European Journal of Law and Economics*, nº33, 2012.

PEERS S., "The data retention judgment: the CJEU prohibits mass surveillance", *EU Law Analysis*, 8 de abril de 2014. Disponible online en: http://eulawanalysis.blogspot.com.es/2014/04/the-data-retention-judgment-cjeu.html (Última visita el 29/06/2015).

POSNER E.A y VERMEULE A., *Terror in the Balance: Security, Liberty, and the Courts*, Oxford University Press, New York, 2007.

QUESADA GÁMEZ, M. y MINCHEVA E., "No Data Without Protection? Re-Thinking Transatlantic Information Exchange for Law Enforcement Purposes After Lisbon", en CARDWELL, P.J., *EU External Relations Law and Policy in the Post-Lisbon Era*, T.M.C. Asser Press, The Hague, 2012.

SALINAS DE FRÍAS, A.M., SAMUEL K.L.H. y WHITE N.D. (eds.), *Counter Terrorism: International Law and Practice,* Oxford University Press, New York, 2012.

SIEBER, U. y BRUNST, P.W., *Cyberterrorism and Other Use of the Internet for Terrorist Purposes: Threat Analysis and Evaluation of International Conventions,* Council of Europe Publishing, 2007.

STEINBERG, G.W., *German Jihad. On the Internationalization of Islamist Terrorism,* Columbia University Press, New York, 2013.

STOEVA. E., "The Data Retention Directive and the right to privacy", *Academy of European Law Forum*, vol. 15, Issue 4, December 2014, pp. 575-592.

THOMAS, T.L., "Al Qaeda and the Internet: The Danger of Cyberplanning", *Parameters,* vol. 23, Issue 1, Spring 2003, pp. 112-123.

WEIMANN. G., "How Modern Terrorism Uses the Internet", *United States Institute of Peace*, Special Report 116, Marzo de 2004.

WEIMAN, G., *Using the Internet for Terrorism Recruitment and Mobilization*, IOS Press, The NATO Science for Peace and Security Programme, Amsterdam, 2007.

Legislación

Carta de Derechos Fundamentales de la Unión Europea, DO C 83/02, 30.3.2010

Decisión Marco 2002/475/JAI del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo, DO L 164/3, 22.06.2002.

Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que se modifica la Decisión 2002/475/JAI sobre la lucha contra el terrorismo, DO L 330/21, 9.12.2008.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281, 23.11.95.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, DO L 178, 17.7.2000.

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 (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201, 31.7.2002.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DO L 105, 13.4.2006.

Jurisprudencia

TJCE, sentencia de 30 de mayo de 2006, *Parlamento Europeo c. Comisión y Consejo*, asuntos acumulados C-317/04 Y C-318/04, Rec. Pág. I-0472.

TJUE, sentencia de 12 de julio de 2011*, L'Oreal c. EBay*, C-324/09, Rec. pág. I-06011,

TJUE, sentencia de 19 de abril de 2012, *Bonnier Audio y otros contra Perfect Communication Sweden AB*, C-461/10, ECLI:EU:C:2012:219.

TJUE, sentencia de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros*, asuntos acumulados C-293/12 y C-594/12, no publicado aún en la Recopilación.

STL*, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, 16 de febrero de 2011, Case No. STL-11/01/I, párs. 83 a 85. Disponible online en: http://www.stl-tsl.org/en/rule-176bis-decision (Última consulta 19.06.2015).

Documentos oficiales e informes

Carta abierta de un grupo de Eurodiputados al Comisario Europeo para el Mercado Interior y Servicios, Michael Barnier, 3.07.2013. Disponible online en: https://ameliaandersdotter.eu/sites/default/files/letter_commissioner_barnier_notice_and_takedown.pdf (Última visita el 29/06/2015).

Consejo de Derechos Humanos de Naciones Unidas, "Illicit financial flows, human

rights and the post-2015 development agenda", A/HRC/28/60, 10 de febrero de 2015, p. 19.
Disponible online en:
http://www.ohchr.org/Documents/Issues/Development/IEDebt/A_HRC_28_60_en.pdf
(Última visita el 29/06/2015).

Comisión Europea, "A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, 4.06.2012-11.09.2012.

Comisión Europea, Comunicación COM(2003) 702 final de 21 de noviembre de 2003: primer informe sobre la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el mercado interior (Directiva sobre el comercio electrónico).

Comisión Europea, Comunicación COM (2010) 673 final al Parlamento Europeo y al Consejo, la Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura, 22 de noviembre de 2010.

Comisión Europea, Comunicación COM(2011) 942 final/2 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Un marco coherente para aumentar la confianza en el mercado único digital del comercio electrónico y los servicios en línea.

Comisión Europea, Comunicación Conjunta JOIN (2013) 1 final al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de ciberseguridad de la Unión Europea: un espacio abierto, protegido y seguro, 7 de febrero de 2013.

Comisión Europea, Comunicación COM (2015) 185 final final al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Agenda Europea de Seguridad, 28 de abril de 2015. Disponible online en:

http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-185-ES-F1-1.PDF (Última visita el 29/06/2015).

Congressional Research Service, "The Economic Effects of 9/11: A retrospective Assesment", 2002.
Disponible online en: http://fas.org/irp/crs/RL31617.pdf (Última visita el 29/06/2015).

Consejo de la Unión Europea, "Conclusiones del Consejo sobre la cooperación en la lucha contra la utilización de Internet por terroristas (Check the web)", 8457/07, 19 de abril de 2007.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-8457-2007-INIT/es/pdf (Última visita el 29/06/2015).

Consejo de la Unión Europea, "Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas", 14781/1/05, 24 de noviembre de 2005.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-14781-2005-REV-1/es/pdf (Última visita el 29/06/2015).

Consejo de la Unión Europea, "Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas – Informe de su aplicación", 15443/07, 23 de noviembre de 2007.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-15443-2007-INIT/es/pdf (Última visita el 29/06/2015).

Consejo de la Unión Europea, "Estrategia Europea de Seguridad", 15895/03, 8 de diciembre de 2003.
Disponible online en: http://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/es/pdf. (Última visita el 29/06/2015).

Consejo de la Unión Europea, "Estrategia de Lucha contra el Terrorismo", 14469/3/05, 30 de noviembre de 2005.
Disponible online en:
http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=es (Última visita el 29/06/2015).

Declaración Conjunta sobre la Libertad de Expresión y las Respuestas a las Situaciones de Conflicto, de 4 de mayo de 1015.

Declaración del Comité de Ministros sobre la libertad de expresión y de información en los medios de comunicación en el contexto de la lucha contra el terrorismo, 2 de marzo de 2005.

Declaración de Riga de los Ministros de Justicia e Interior de la UE. Disponible online en: https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf (Última visita el 29/06/2015).

Declaración del Consejo Europeo sobre la lucha contra el terrorismo, 29.03.2004. Disponible online en: http://data.consilium.europa.eu/doc/document/ST-7906-2004-INIT/es/pdf (Última visita el 29/06/2015).

European Digital Rights, Informe de Consulta Pública. Disponible online en: https://edri.org/files/057862048281124912Submission_EDRi_NoticeAction.pdf (Última visita el 29/06/2015).

Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2014. Disponible online en: https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014 (Última visita el 29/06/2015).

House of Representatives, "Progress since 9/11: the effectiveness of the U.S. anti-terrorist financing efforts : hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services", One Hundred Eighth Congress, first session, March 11, 2003.

International Institute for Counter-Terrorism, "Cyber-Terrorism Activities", Reports nº 10 y 11.

Memorandum of Understanding, 4 May 2011, Brussels. Disponible online en: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (Última visita el 29/06/2015).

Propuesta de Resolución Común del Parlamento Europeo sobre las medidas de lucha contra el terrorismo, RC-B8-0122/2015, 10.2.2015, pár. 19.

United Nations Office on Drugs And Crime, *The use of Internet for Terrorist Purposes*, United Nations Office, Viena, 2012.

Artículos periodísticos y notas de prensa

ROSE, S., "The Isis propaganda war: a hi-tech media jihad", The Guardian, 7 de octubre de 2014.
Disponible online en: http://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war (Última visita el 29/06/2015).

FLEMING, J., "EU lawmaker warns of data protection rules delay till 2016", *EurActiv.com*, 14 de enero de 2015. Disponible online en http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100 (Última visita el 29/06/2015).

Comisión Europea, "Apoyo de los ministros de Justicia a la propuesta de la Comisión de fijar nuevas normas de protección de datos para impulsar el mercado único digital de la UE", Comunicado de Prensa, 15 de junio de 2015. Disponible online en: http://europa.eu/rapid/press-release_IP-15-5176_es.htm (Última visita el 29/06/2015).

Comisión Europea, "European Parliament backs stronger rules to combat money laundering and terrorism financing", *Press Release*, 20 May 2015.