

UNIVERSIDAD DE GRANADA



TESIS DOCTORAL:
LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA
CON RELACIÓN AL
TERRORISMO YIHADISTA EN INTERNET
de
GILDA B. GADEA ALDAVE

Director:
PROF. DR. DR. MIGUEL ÁNGEL CANO PAÑOS

UNIVERSIDAD DE GRANADA
PROGRAMA DOCTORAL EN CRIMINOLOGÍA
LÍNEA DE INVESTIGACIÓN: CIBERCRIMINALIDAD Y DELINCUENCIA TRANSNACIONAL

Granada, 2024

Editor: Universidad de Granada. Tesis Doctorales
Autor: Gilda Beatriz Gadea Aldave
ISBN: 978-84-1195-562-1
URI: <https://hdl.handle.net/10481/97438>

DEDICATORIAS

Para mi madre,
la Sra. Elsa Beatriz Aldave de Gadea,
la persona más perseverante que el cielo o la tierra haya conocido nunca.

Para Mercedes,
por creer en mí.

AGRADECIMIENTOS

A mi director, tutor y guía,
el Prof. Dr. Dr. (Potsdam), LL.M. (Münster) Miguel Ángel Cano Paños
por su invaluable orientación en un campo científico tan relevante como es la Criminología,
y por sus excelentes aportes adyacentes sobre el
Derecho penal español, europeo e internacional.
Admiro su gran conocimiento y su facultad para transmitirlo con pasión
con una visión académica apegada a la protección de los derechos humanos.
Gracias por todas nuestras conversaciones.

A la Prof. Dr. Dr. h.c., LL.M. (Harvard). Anne Peters,
Directora del
Max Planck Institute for Comparative Public Law and International Law de Heidelberg,
por autorizar mi visita al centro de investigación y por facilitar durante un mes,
y en el marco de esta tesis, mi aprendizaje sobre el Derecho Internacional Comparado.

Al Prof. Dr. Dr. h.c. mult. Hans-Jörg Albrecht,
Director emérito del
Max Planck Institute for the Study of Crime, Security and Law de Freiburg,
por abrirme la puerta, durante dos meses, a uno de los acervos bibliográficos
más importantes en el mundo sobre el Derecho penal y la Criminología.

A la Prof. Dra. María Inmaculada Ramos Tapia,
Directora de mi
Trabajo de Fin de Master en Derecho Internacional y Relaciones Internacionales,
por sus tempranas y sólidas enseñanzas sobre el Derecho penal europeo,
y por haber dirigido mi primer estudio académico sobre el terrorismo.
Agradecerle también el presentarme al Profesor Dr. Dr. Miguel Ángel Cano Paños y
recomendarlo como el experto más adecuado para la dirección de esta tesis doctoral.

TESIS DOCTORAL

LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON
RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET
de
GILDA B. GADEA ALDAVE

PhD THESIS

CRIMINAL POLICY OF THE EUROPEAN UNION IN RELATION
TO JIHADIST TERRORISM ON THE INTERNET
by
GILDA B. GADEA-ALDAVE

INDICE

RESUMEN: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET	7
RESUME: CRIMINAL POLICY OF THE EUROPEAN UNION IN RELATION TO JIHADIST TERRORISM ON THE INTERNET	9
ABREVIATURAS.....	11
PLANTEAMIENTO DE LA INVESTIGACIÓN	16
OBJETIVOS, DESCRIPCIÓN Y DELIMITACIÓN DEL ESTUDIO.....	16
JUSTIFICACIÓN.....	19
METODOLOGÍA	20
INTRODUCCIÓN.....	23
PARTE I: TERRORISMO Y TERRORISMO YIHADISTA	27
CAPÍTULO 1: EL FENÓMENO DEL TERRORISMO INTERNACIONAL.....	27
CAPÍTULO 2: INTERNET COMO EL ESPACIO IDÓNEO PARA UNA NUEVA OPORTUNIDAD CRIMINAL	37
CAPÍTULO 3: EL USO YIHADISTA DE INTERNET Y LA E-YIHAD DEL AUTOPROCLAMADO ESTADO ISLAMICO.....	52
PARTE II: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET	73
CAPÍTULO 4: LA POLÍTICA CRIMINAL DE LA UE ANTE EL YIHADISMO ONLINE	73
<i>DEFINIENDO EL CONCEPTO DE POLÍTICA CRIMINAL</i>	<i>73</i>
<i>EL TERRORISMO YIHADISTA EN INTERNET ENTENDIDO COMO UN GRAVE PROBLEMA DE SEGURIDAD EUROPEO Y LA POLÍTICA COMÚN DE SEGURIDAD Y DEFENSA (PCSD) DE LA UE EN REFERENCIA A ESTE FENÓMENO</i>	<i>86</i>
CAPÍTULO 5: MEDIDAS NORMATIVAS EUROPEAS ORIENTADAS A LA PERSECUCIÓN DEL USO DE INTERNET CON FINES YIHADISTAS	102
<i>EL DERECHO DE LA UNIÓN EUROPEA COMO ORDENAMIENTO JURIDICO PROPIO</i>	<i>102</i>
<i>DERECHO DE LA UNIÓN EUROPEA REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS</i>	<i>106</i>
<i>DERECHO DEL CONSEJO DE EUROPA REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS</i>	<i>113</i>
<i>LA INFLUENCIA DEL DERECHO INTERNACIONAL REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS.....</i>	<i>118</i>
CAPÍTULO 6: MEDIDAS INSTITUCIONALES DE LA UNIÓN EUROPEA TENDIENTES A LA COOPERACIÓN EN EL CONTROL Y VIGILANCIA DE INTERNET Y A LA REPRESIÓN SOBRE SU USO CON FINES YIHADISTAS	123
<i>LA COOPERACIÓN EUROPEA INSTITUCIONALIZADA REFERENTE AL USO DE INTERNET CON FINES YIHADISTAS</i>	<i>123</i>
<i>MEDIDAS DE VIGILANCIA Y CONTROL DE INTERNET.....</i>	<i>130</i>
CAPÍTULO 7: MEDIDAS PREVENTIVAS EUROPEAS DESTINADAS A EVITAR EL RECLUTAMIENTO YIHADISTA ONLINE Y LOS EXTREMISMOS EN INTERNET.....	154
<i>LA PREVENCIÓN DEL TERRORISMO MEDIANTE EL DISEÑO DE POLÍTICAS PÚBLICAS.....</i>	<i>154</i>
<i>LAS MEDIDAS DE INTERVENCIÓN, LAS CAMPAÑAS DE INFORMACIÓN Y LAS ACCIONES DE CONTRANARRATIVA YIHADISTA EN INTERNET ADOPTADAS DENTRO DE LA UNIÓN EUROPEA.</i>	<i>164</i>

PARTE III: REVISIÓN COMPARADA DE LA POLÍTICA CRIMINAL DE TRES ESTADOS EUROPEOS REFERENTE AL USO DE INTERNET CON FINES TERRORISTAS.....	174
CAPÍTULO 8: ALEMANIA	174
<i>LA POLÍTICA CRIMINAL DE ALEMANIA EN MATERIA DE TERRORISMO</i>	<i>174</i>
<i>LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL ALEMANA..</i>	<i>180</i>
CAPÍTULO 9: REINO UNIDO	194
<i>LA POLÍTICA CRIMINAL DE REINO UNIDO EN MATERIA DE TERRORISMO</i>	<i>194</i>
<i>LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL BRITANICA</i>	<i>195</i>
CAPÍTULO 10: ESPAÑA	223
<i>LA POLÍTICA CRIMINAL DE ESPAÑA EN MATERIA DE TERRORISMO</i>	<i>223</i>
<i>LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL ESPAÑOLA</i>	<i>228</i>
CONCLUSIONES Y PROPUESTAS PARA FOMENTAR LA ARMONIZACIÓN DE LA POLÍTICA CRIMINAL EN LA UNIÓN EUROPEA EN MATERIA DE TERRORISMO EN INTERNET	250
CONCLUSIONS AND PROPOSALS TO PROMOTE THE HARMONIZATION OF CRIMINAL POLICY IN THE EUROPEAN UNION REGARDING TERRORISM ON THE INTERNET	260
BIBLIOGRAFÍA.....	270
GLOSARIO INSTITUCIONAL DE LA POLÍTICA CRIMINAL DE LA UE	305
AGENCIAS EUROPEAS	305
AR (ALTO REPRESENTANTE DE LA UE PARA ASUNTOS EXTERIORES Y POLÍTICA DE SEGURIDAD).....	305
CEPOL (AGENCIA DE LA UNIÓN EUROPEA PARA LA FORMACIÓN POLICIAL)	306
CoE (CONSEJO DE EUROPA)	307
CONSEJO DE LA UNIÓN EUROPEA	308
CONSEJO EUROPEO	309
ECTC (CENTRO EUROPEO CONTRA EL TERRORISMO)	310
EDA (AGENCIA EUROPEA DE DEFENSA)	312
EEMM (ESTADO/S MIEMBRO/S).....	312
ENISA (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD)	313
EU INCEN (CENTRO DE INTELIGENCIA Y SITUACIÓN DE LA UE).....	314
EU IRU (UNIDAD DE REFERENCIA DE LA UNIÓN EUROPEA)	316
EUROJUST (AGENCIA DE LA UNIÓN EUROPEA PARA LA COOPERACIÓN JUDICIAL PENAL)....	316
EUROPOL (AGENCIA DE LA UNIÓN EUROPEA PARA LA COOPERACIÓN POLICIAL)	317
EUROSUR (SISTEMA EUROPEO DE VIGILANCIA DE FRONTERAS).....	319
FRONTEX (AGENCIA EUROPEA DE LA GUARDIA DE FRONTERAS Y COSTAS)	320
PARLAMENTO EUROPEO	321
RJE (RED JUDICIAL EUROPEA EN MATERIA PENAL).....	323
SITCEN (CENTRO CONJUNTO DE SITUACIÓN DE LA UNIÓN EUROPEA)	324
SEAE (SERVICIO EUROPEO DE ACCION EXTERIOR).....	324
ANEXOS	325
ANEXO N.º 01: ORIGEN Y EVOLUCIÓN DE LA UNIÓN EUROPEA	325
ANEXO N.º 02: DOCUMENTO PÚBLICO DE FUNCIONAMIENTO INTERNO DE PERCI.....	342
ANEXO N.º 03: ENTREVISTA CON UN FUNCIONARIO DE LA UNIDAD DE REFERENCIA DE INTERNET DE LA UE DE EUROPOL [versión original y traducción al castellano].	351
ANEXO N.º 04: COMUNICADO DE PRENSA: LEY DE SERVICIOS DIGITALES: ENTRAN EN VIGOR LAS NORMAS DETERMINANTES DE LA UE PARA LAS PLATAFORMAS EN LÍNEA.	367
ANEXO N.º 05: MEDIDAS CONTRA LA RADICALIZACIÓN FINANCIADAS POR LA UE.....	371

RESUMEN: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET

El delito de terrorismo siempre ha sido considerado uno de los delitos de especial gravedad debido a que su finalidad es subvertir el orden constitucionalmente establecido, por medio la violencia. El principal objetivo que busca el terrorismo es la erradicación y afectación total del Estado o el debilitamiento de sus instituciones políticas, de su estructura económica y de su entramado social.

Tras el 11-S, con los ataques a las Torres Gemelas de Nueva York, el terrorismo yihadista pasó a convertirse en un fenómeno transnacional. De un terrorismo doméstico que afectaba a una población determinada y local pasó a ser un terrorismo foráneo que podía hacer sentir sus efectos más allá de su territorio de origen.

Años después, con la democratización del uso de Internet, se inicia un proceso de traslación del delito de terrorismo hacia el mundo virtual. Este terrorismo en Internet no sustituye al terrorismo tradicional, sino que lo refuerza y lo acrecienta debido a que Internet potencia y multiplica el efecto y el alcance de las acciones terroristas. Este nuevo terrorismo, de origen primordialmente yihadista, se acelera en Internet por medio de los diferentes usos que el terrorismo hace de la red. Internet le permite al terrorismo yihadista desarrollar un gran aparato discursivo con fines de captación, de promoción a la incitación del terrorismo y de radicalización. Además, Internet le permite al terrorismo incrementar la funcionalidad interna de su organización y la eficacia de sus atentados, debido a que funciona también como una herramienta operativa de actuación criminal.

Con el surgimiento de Internet, el terrorismo yihadista alcanzó una dimensión sin precedentes porque tuvo impacto en cuatro grandes aspectos. Con Internet las organizaciones yihadistas desarrollaron un crecimiento exponencial debido a que se multiplicaron en todo el mundo las cuotas de reclutamiento de nuevos miembros. Con Internet el yihadismo puede ahora explorar otras formas criminales derivadas del uso de la Tecnología Informática. Con Internet la comisión del crimen de terrorismo adquiere una autonomía, un anonimato y una internacionalización que dificulta su persecución penal. Con Internet el delito de terrorismo ya no solo es una forma grave de criminalidad, sino que también representa una amenaza para todo el Sistema internacional.

Todo este escenario ha hecho que el terrorismo yihadista en Internet comenzara a ser observado como un grave problema transnacional que debiera ser atendido de forma conjunta por todas las partes afectadas. La respuesta de la comunidad internacional en la lucha contra el terrorismo yihadista resultó decisiva para establecer el marco de actuación cooperativa entre todos los Estados del globo.

En sintonía con este contexto, la Unión Europea, comienza a desarrollar respuestas propias que le permitan combatir todos aquellos delitos de terrorismo que tienen lugar dentro de su espacio comunitario, y concede especial interés a aquellos delitos de terrorismo que se comentan mediante el uso de Internet.

Si bien el terrorismo no representaba ninguna novedad, la adecuaciones modernas que permitió Internet sobre esta forma criminal sí que lo eran. El nuevo panorama delictivo que estableció de facto el uso de Internet por parte del terrorismo dinamizó la necesidad de crear medidas normativas, operativas y preventivas que permitan luchar contra este tipo de delincuencia. La adopción de estas nuevas medidas, desarrolladas a lo largo de la última década, han ido perfilando la Política Criminal de la Unión Europea frente a este fenómeno.

¿Cómo es la Política Criminal de la Unión Europea en cuanto al terrorismo yihadista en Internet?, ¿Es la Política Criminal de la Unión Europea equivalente a la de sus Estados Miembros?, ¿Cuenta la Política Criminal de la Unión Europea con medidas eficaces para reprimir este tipo de delincuencia?, ¿Cuáles son las diferentes instituciones y agencias europeas que intervienen en la lucha contra este fenómeno?, ¿Cómo se articula la cooperación judicial y policial dentro del espacio Schengen?, ¿Cuenta la Unión Europea con normativa actualizada que permita actuaciones eficaces?, ¿En qué consisten las acciones preventivas de la Unión Europea para luchar contra el terrorismo yihadista en Internet?.

Estas son algunas de las preguntas a las que esta tesis doctoral busca dar respuesta.

RESUME: CRIMINAL POLICY OF THE EUROPEAN UNION IN RELATION TO JIHADIST TERRORISM ON THE INTERNET

The crime of terrorism has always been considered one of the especially serious crimes because its purpose is to subvert the constitutionally established order, through violence. The main objective pursued by terrorism is the eradication and total impact of the State or the weakening of its political institutions, its economic structure and its social fabric.

After 9/11, with the attacks on the Twin Towers in New York, jihadist terrorism became a transnational phenomenon. From internal terrorism that affected a specific and local population, we move on to external terrorism that could make its effects felt beyond its territory.

Years later, with the democratization of the Internet, a process began that moved the crime of terrorism to the virtual world. This Internet terrorism does not replace traditional terrorism but rather reinforces and increases it because the Internet enhances and multiplies the effect and scope of terrorist actions. This new terrorism, of jihadist origin, accelerates on the Internet through the different uses that terrorism makes of the network. The Internet allows jihadist terrorism to develop a large discursive apparatus for the purposes of recruitment, incitement of terrorism and radicalization. In addition, the Internet allows terrorism to increase the internal functionality of its organization and the efficiency of its attacks, because it functions as an operational tool for criminal action.

With the Internet, jihadist terrorism reached an unprecedented dimension because it had an impact in four major aspects. With the Internet, jihadist organizations developed exponential growth because the recruitment of new members multiplied throughout the world. With the Internet, jihadism can now explore other criminal forms derived from the use of Information Technology. With the Internet, the crime of terrorism adopts an autonomy, anonymity and an internationalization that makes criminal prosecution difficult. With the Internet, the crime of terrorism is no longer only a serious form of crime, but also represents a threat to the entire International System.

This entire scenario has meant that jihadism on the Internet began to be observed as a serious transnational problem that should be resolved jointly by all affected parties. The response of the international community in the fight against jihadism was fundamental to establish the framework for cooperative action between all the States of the world.

In line with this context, the European Union is beginning to develop its own responses to combat all terrorist crimes that take place in its common territory and gives special attention to those terrorist crimes that are committed through the Internet.

While terrorism was nothing new, the modern adaptations that the Internet enabled to this form of crime were. The new criminal panorama established with the Internet by terrorism stimulated the need to create laws and operational and preventive measures that allow to fight this crime. The adoption of these new measures, created over the last decade, have been shaping the Criminal Policy of the European Union against this phenomenon.

What is the Criminal Policy of the European Union regarding jihadism on the Internet? Is the Criminal Policy of the European Union equivalent to the Criminal Policy of its Member States? Does the EU Criminal Policy have effective measures to repress this crime? What are the European institutions and agencies that participate in the fight against this phenomenon? How is judicial and police cooperation organized within the Schengen area? Does the European Union have current regulations that allow effective actions? What are the preventive actions of the European Union to fight against jihadist terrorism on the Internet?

These are some of the questions that this PhD thesis seeks to answer.

ABREVIATURAS

9/11	Atentados del 11 de septiembre de 2001 en Estados Unidos de América (numerónimo de EEUU y A. Latina)
11-M	Atentado del 11 de marzo de 2004 en Atocha, España
11-S	Atentados del 11 de septiembre de 2001 en Estados Unidos de América (numerónimo de España)
17-A	Atentados del 17 de agosto de 2017 en Barcelona y Cambrils, Cataluña
AA	American Airlines
ACPO	Association of Chief Police Officers of England, Wales and Northern Ireland (Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte) [GBR]
ACT	Action Counters Terrorism (Acción Contra el Terrorismo) [GBR]
AI	Inteligencia Artificial
AIDA	Applied Intelligence and Data Analysis (Inteligencia Aplicada y Análisis de Datos)
AR	Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad [UE]
ATCS	Anti-Terrorism, Crime and Security (Ley contra el Terrorismo, la Delincuencia y la Seguridad) [GBR]
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives (Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos) [EEUU]
AWF	Ficheros de Análisis
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Autoridad Federal de Supervisión Financiera) [DEU]
B.C.I.T.	Brigada Central de Investigación Tecnológica (ESP)
BEL	Bélgica
BfV	Bundesamt für Verfassungsschutz (Oficina Federal para la Protección de la Constitución) [DEU]
BGH	Bundesgerichtshof (Tribunal Federal de Justicia) [DEU]
BKA	Bundeskriminalamt (Oficina Federal de Policía Criminal) [DEU]
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend (Ministerio Federal de Familia, Tercera Edad, Mujeres y Juventud) [DEU]
BND	Bundesnachrichtendienst (Servicio Federal de Inteligencia) [DEU]
BNDG	Gesetz über den Bundesnachrichtendienst, BND-Gesetz (Ley del Servicio Federal de Inteligencia) [DEU]
BPol	Bundespolizei (Policía Federal) [DEU]
BPolG	Bundespolizeigesetz (Ley de la Policía Federal) [DEU]
BZRG	Bundeszentralregistergesetz (Ley del Registro Central Federal) [DEU]
CARD	Annual Coordinated Defense Review (Revisión Anual Coordinada de la Defensa) [UE]
CBP	Customs and Border Protection (Aduanas y Protección Fronteriza) [EEUU]
CBRN-E	Chemical, biological, radiological and nuclear substances and explosives (Sustancias y explosivos químicos, biológicos, radiológicos y nucleares)
CCIR	Centro de Coordinación de Información sobre la Radicalización [ESP]
CEPOL	(ex) Collège Européen de Police (Agencia de la Unión Europea para la Formación Policial) [UE]
CPTED	Crime Prevention Through Environmental Design (Prevención del delito mediante el diseño ambiental)
CEV	Combatir Extremismo Violento
CFSP	Common Foreign and Security Policy (<i>idem</i> PESC) [UE]
C.G.P.J.	Comisaría General de Policía Judicial [ESP]
CGPJ	Consejo General del Poder Judicial [ESP]
CISA	Cybersecurity and Infrastructure Security Agency (Agencia de Seguridad de Infraestructura y Ciberseguridad) [EEUU]
CITCO	Centro de Inteligencia contra el Terrorismo y del Crimen Organizado del Ministerio del Interior [ESP]
CNI	Centro Nacional de Inteligencia [ESP]
CNI	Critical National Infrastructure (Infraestructura Nacional Crítica) [GBR]
C.N.P.	Cuerpo Nacional de Policía [ESP]
CoCoRa	Community Counteracting Radicalisation (Comunidad Contra la Radicalización) [ITA]
CoE	Council of Europe (Consejo de Europa)
CoPPRa	Community Policing Preventing Radicalisation (Vigilancia Comunitaria para Prevenir la Radicalización) [UE]
COSI	Standing Committee on Operational Cooperation on Internal Security (Comité permanente de Cooperación Operativa en materia de Seguridad Interior) [UE]
CP	Código Penal [ESP]

CPNI	Centre for the Protection of National Infrastructure (Centro para la Protección de la Infraestructura Nacional) [GBR]
CPTED	Crime Prevention Through Environmental Design (Prevención del Delito mediante el Diseño Ambiental)
CSAM	Child Sexual Abuse Material (Material sobre abuso sexual infantil)
CCSC	Center for Strategic Counterterrorism Communications (Centro de Comunicaciones Estratégicas Antiterroristas) [EEUU]
CSDP	Common Security and Defense Policy (Política Común de Seguridad y Defensa) [UE]
CTA	Common Travel Area (Área Común de Viaje) [GBR]
CTC	Combating Terrorism Center at West Point (Centro de Lucha contra el Terrorismo de West Point) [EEUU]
CTIRU	Counter-Terrorism Internet Referral Unit (Unidad de Referencia de Internet contra el Terrorismo) [GBR]
CTP	Counter Terrorism Policing (Policía Antiterrorista) [GBR]
CTPN	Counter Terrorism Preparedness Network (Red de Preparación contra el Terrorismo) [GBR]
CTSA	Counter Terrorism Security Adviser (Asesores de Seguridad contra el Terrorismo) [GBR]
CtW	Check the Web
Dáesh	al-Dawla al-Islamiya al-Iraq al-Sham (Estado Islámico de Irak y el Levante)
DDAT	Departamento de Delitos de Alta Tecnología [ESP]
DEA	Drug Enforcement Administration (Administración de Control de Drogas) [EEUU]
DEU	Deutschland (Alemania)
DM	Decisión Marco [UE]
DOUE	Diario Oficial de la Unión Europea [UE]
DSA	Digital Services Act (Ley de Servicios Digitales) [UE]
DSN	Departamento de Seguridad Nacional [ESP]
DSS	Diplomatic Security Service (Servicio de Seguridad Diplomática) [EEUU]
DUE	Derecho de la Unión Europea [UE]
EAW	European Arrest Warrant (<i>idem</i> EUROORDEN) [UE]
EDA	European Defense Agency (Agencia Europea de Defensa) [UE]
EDF	European Defense Fund (Fondo Europeo de Defensa) [UE]
EEAS	European Union External Action (<i>idem</i> SEAE) [UE]
EEMM	Estado/s Miembro/s
EES	Estrategia Europea de Seguridad [UE]
EEUU	Estados Unidos de América
ECAT	European Centre for Algorithmic Transparency (Centro Europeo para la Transparencia Algorítmica) [UE]
ECCRI CIC	European Cyber Conflict Research Incubator (Incubadora Europea de Investigación sobre conflictos cibernéticos) [GBR]
ECTC	European Counter-Terrorism Centre (Centro Europeo Contra el Terrorismo) [UE]
EC3	European Cybercrime Centre (Centro Europeo de Ciberdelincuencia) [UE]
EDITE,s	Equipos de Investigación Tecnológica [ESP]
EI	Estado Islámico (Autoproclamado)
EIIL	Estado Islámico de Irak y el Levante
EIIS	Estado Islámico de Irak y Siria
ENISA	European Union Agency for Network and Information Security (Agencia de la Unión Europea para la Ciberseguridad) [UE]
EPF	European Peace Support Fund (Fondo Europeo de Apoyo a la Paz) [UE]
ESCN	European Strategic Communication Network (Red Europea de Comunicación Estratégica) [UE]
ESN	Estrategia de Seguridad Nacional [EEUU]
ESP	España
ETA	Euskadi Ta Askatasuna (Patria Vasca y Libertad)
ETIAS	European Travel Information and Authorisation System (Sistema Europeo de Información y Autorización de Viajes) [UE]
EU BGs	EU Battlegroups (Agrupaciones Tácticas de Reacción Rápida) [UE]
EUIF	European Union Internet Forum (Foro de Internet de la Unión Europea) [UE]
EU INTCE	EU Intelligence and Situation Centre (Centro de Inteligencia y Situación de la Unión Europea) [UE]
EU IRU	EU Internet Referral Unit (Unidad de Referencia de Internet de la Unión Europea) [UE]
EUMS	European Union Military Staff (Estado Mayor de la Unión Europea) [UE]
EUROJUST	European Union Agency for Criminal Justice Cooperation (Agencia de la Unión Europea para la Cooperación Judicial Penal) [UE]
EUROORDEN	Orden Europea de Detención y Entrega [UE]
EUROSUR	European Border Surveillance System (Sistema Europeo de Vigilancia de Fronteras) [UE]

EUROPOL	European Union Agency for Law Enforcement Cooperation (Agencia de la Unión Europea para la Cooperación Policial) [UE]
FATF	Financial Action Task Force (Grupo de Acción Financiera Internacional)
FBI	Federal Bureau of Investigation (Oficina Federal de Investigaciones) [EEUU]
FDA	Food and Drug Administration (Administración de Alimentos y Medicamentos) [EEUU]
FinCEN	Financial Crimes Enforcement Network (Red de Control de Delitos Financieros) [EEUU]
FRONTEX	European Border and Coast Guard Agency (Agencia Europea de la Guardia de Fronteras y Costas) [UE]
GBA	Generalbundesanwalt (Procurador/Fiscal General) [DEU]
GBR	Great Britain (Gran Bretaña)
GDI	Grupo de Delitos Informáticos [ESP]
GDT	Grupo de Delitos Telemáticos de la Guardia Civil [ESP]
GEC	Global Engagement Center (Centro de Participación Global, - ex CSCC -) [EEUU]
G.E.O.	Grupo Especial de Operaciones [ESP]
GIFCT	Global Internet Forum to Counter Terrorism (Foro Mundial de Internet sobre la Lucha contra el Terrorismo)
GPS	Global Positioning System (Sistema de Posicionamiento Global)
GSEC	Google Security Engineering Center (Centro de Ingeniería de Seguridad de Google)
GTAZ	Gemeinsames Terrorismusabwehrzentrum (Centro Conjunto Contra el Terrorismo) [DEU]
GTI	Global Terrorism Index (Índice Global de Terrorismo)
GVVG	Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (Ley sobre el Procesamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado) [DEU]
GVVG-ÄndG	Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (Ley de Enmienda sobre el Enjuiciamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado) [DEU]
HM	Her/His Majesty (Su Majestad) [GBR]
HMG	Her/His Majesty's Government (Gobierno de Reino Unido) [GBR]
HO	Home Office (Ministerio del Interior) [GBR]
HR	High Representative of the Union for Foreign Affairs and Security Policy (<i>idem</i> AR) [UE]
HUMINT	Human Intelligence (Inteligencia Humana)
IC3	Crime Complaint Center (Centro Europeo de Cibercrimen) [UE]
ICCT	International Centre for Counter-Terrorism (Centro Internacional de Lucha contra el Terrorismo) [UE]
ICE	Immigration and Customs Enforcement (Servicio de Inmigración y Control de Aduanas) [EEUU]
IOCTA	Internet Organised Crime Threat Assessment (Informe de Evaluación de la Amenaza del Crimen Organizado en Internet) [UE]
IP	Internet Protocol
IRA	Irish Republican Army (Ejército Republicano Irlandés)
IRB	Irish Republican Brotherhood (Hermandad Republicana Irlandesa)
IRS	Internal Revenue Service (Servicio de Impuestos Internos) [EEUU]
IS	Islamic State (self-named)
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
ITA	Italia
JAI	Consejo de Justicia y Asuntos de Interior de la Unión Europea [UE]
J-CAT	Joint Cybercrime Action Taskforce (Grupo de Trabajo Conjunto de Acción contra el Cibercrimen) [UE]
JHA	Justice and Home Affairs Council (<i>idem</i> JAI) [UE]
JSaRC	Joint Security and Resilience Centre (Centro Conjunto de Seguridad y Resiliencia) [GBR]
JTAC	Joint Terrorism Analysis Centre (Centro Conjunto de Análisis del Terrorismo) [GBR]
KIgA	Kreuzberg Initiative against Antisemitism (Iniciativa Kreuzberg contra el antisemitismo) [DEU]
LKA	Landeskriminalämter (Oficinas de Policía Criminal del Land) [DEU]
LO	Ley Orgánica [ESP]
LuftVG	Luftverkehrsgesetz (Ley de aviación) [DEU]
MAC	Multi-Agency Centre (Centro Multiagencia) [GBR]
MAD	Millitärischer Abschirmdienst (Servicio de Contrainteligencia Militar) [DEU]
MAKS VZW	Media Actie Kuregem Stad (Acción Mediática de la Ciudad de Kuregem) [BEL]
MI5	Security Service (Servicio de Seguridad) [GBR]
MoJ	Ministry of Justice (Ministerio de Justicia) [GBR]
MoU	UK - Ireland Memorandum of Understanding (Memorandum de Entendimiento entre Reino Unido e Irlanda) [GBR]
NaCTSO	National Counter Terrorism Security Office (Oficina de Seguridad y Contraterrorismo) [GBR]

NCA	National Crime Agency (Agencia Nacional contra el Crimen) [GBR]
NCSC	National Cyber Security Centre (Centro Nacional de Seguridad Cibernética) [GBR]
NDES	National Digital Exploitation Service (Servicio Nacional de Explotación Digital) [GBR]
NEV	Narrativas Extremistas de carácter Violento
NLO Network	National Liaison Officers Network (Red Nacional de Oficiales de Enlace) [UE]
NPCC	National Police Chiefs' Council (Consejo de Jefes de Policía Nacional) [GBR]
NPSA	National Protective Security Authority (Autoridad Nacional de Protección y Seguridad) [GBR]
NRF	NATO Response Force (Fuerza de Respuesta de la OTAN)
NSS	National Security Strategy (Estrategia de Seguridad Nacional) [GBR]
NYPD	New York Police Department (Departamento de Policía de Nueva York) [EEUU]
OCDE	Organización para la Cooperación y el Desarrollo Económico
OEDE	Orden Europea de Detención y Entrega (<i>idem</i> EUROORDEN) [UE]
OOII	Organización/es Internacional/es
OLG	Oberlandesgerichte (Tribunales Regionales Superiores) [DEU]
ONGD	Organización No Gubernamental de Desarrollo
ONU	Organización de las Naciones Unidas
OSCE	Organización para la Seguridad y la Cooperación en Europa
OSINT	Open Source Intelligence (Inteligencia de Fuentes Abiertas)
OTAN	Organización del Tratado del Atlántico Norte
PassG	Paßgesetz, PaßG (Ley de pasaportes) [DEU]
PAuswG	Personalausweisgesetz (Ley de cédulas de identidad) [DEU]
PEO	Prevent Education Officer (Oficial de Educación Preventiva) [GBR]
PERCI	Plateforme Européenne de Retraits de Contenus illégaux sur Internet (Plataforma Europea para Eliminar Contenidos Ilegales en Internet) [UE]
PC	Política Criminal
PCA	Política Criminal Aplicada
P/CEV	Prevenir y Combatir el Extremismo Violento
PEN-LCRV	Plan Estratégico Nacional de Lucha contra la Radicalización Violenta [ESP]
PESC	Política Exterior y de Seguridad Común de la Unión Europea [UE]
PESCO	Permanent Structured Cooperation (Cooperación Estructurada Permanente) [UE]
PESD	European Security and Defense Policy (Política Europea de Seguridad y Defensa) [UE]
PEV	Prevenir Extremismo Violento
PMAP	Prevent Multi-Agency Panel (Panel Multi-Agencia de Prevenir, – ex PPC -) [GBR]
PPC	Prevent Professional Concerns (Prevenir Preocupaciones Profesionales) [GBR]
PSC	Political and Security Committee (Comité Político y de Seguridad) [UE]
QC	Queen's Counsel (Consejero de la Reina) [GBR]
RAF	Rote Armee Fraktion (Fracción del Ejército Rojo)
RAD	Referral Action Day (Día de Acción de Referencia)
RAN	Radicalization Awareness Network (Red de Sensibilización sobre la Radicalización) [UE]
RICU	Research, Information and Communications Unit (Unidad de Investigación, Información y Comunicaciones) [GBR]
RJE	Red Judicial Europea [UE]
SDSR	Strategic Defense and Security Review (Revisión de Seguridad y Defensa Estratégica) [GBR]
SEAE	Servicio Europeo de Acción Exterior [UE]
SIA	Security Industry Authority (Autoridad de la Industria de Seguridad) [GBR]
SIAC	Single Intelligence Analysis Capacity (Capacidad Única de Análisis de Inteligencia) [UE]
SIENA	Secure Information Exchange Network Application (Red de Intercambio Seguro de Información) [UE]
SIRIUS	Cross-Border Access to Electronic Evidence (Acceso Transfronterizo a la Prueba Electrónica) [UE]
SITCEN	Joint Situation Centre (Centro Conjunto de Situación de la Unión Europea) [UE]
SSCAT	Syria Strategic Communication Advisory Team (Equipo Asesor de Comunicación Estratégica de Siria) [UE]
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen, Sicherheitsüberprüfungsgesetz (Ley sobre los requisitos y el procedimiento para los controles federales de seguridad y la protección de información clasificada, Ley de Control de Seguridad) [DEU]
TAC	Teoría de las Actividades Cotidianas
TBG	Gesetz zur Bekämpfung des internationalen Terrorismus, Terrorismusbekämpfungsgesetz (Ley de Lucha contra el Terrorismo Internacional) [DEU]
TEDAX	Técnicos Especialistas en Desactivación de Artefactos Explosivos [ESP]

TE-SAT	UE Terrorism Situation & Trend Report (Informe sobre la situación y las tendencias del terrorismo en la Unión Europea) [UE]
TFUE	Tratado de Funcionamiento de la Unión Europea [UE]
TJUE	Tribunal de Justicia de la Unión Europea [UE]
TI	Tecnología Informática
TIC	Tecnologías de la Información y la Comunicación
TSA	Transportation Security Administration (Administración de Seguridad del Transporte) [EEUU]
TUE	Tratado de la Unión Europea [UE]
UA	United Airlines
UAO	Unidad de Apoyo Operativo [ESP]
UCI	Unidad Central de Inteligencia [ESP]
UCIE	Unidad Central de Información Exterior [ESP]
UCIO	Unidad Central de Información Interior [ESP]
UCOA	Unidad Central Operativa Antiterrorista [ESP]
UE	Unión Europea
U.I.T.	Unidad de Investigación Tecnológica [ESP]
UNED	Universidad Nacional de Educación a Distancia
UNODC	United Nations Office on Drugs and Crime (Oficina Contra la Droga y el Delito de las Naciones Unidas)
USSS	United States Secret Service (Servicio Secreto de los Estados Unidos) [EEUU]
VoIP	Voice over Internet Protocol
VP	Vicepresidente de la Comisión Europea [UE]
WTC	World Trade Center
ZIT	Zentrum für islamische Theologie (Centro de Teología Islámica) [DEU]

PLANTEAMIENTO DE LA INVESTIGACIÓN

OBJETIVOS, DESCRIPCIÓN Y DELIMITACIÓN DEL ESTUDIO

Esta investigación doctoral estudia la Política Criminal de la Unión Europea (UE) referente al terrorismo yihadista en Internet, y propone como caso de estudio una revisión comparada de la Política Criminal de tres Estados de Europa en relación con el mismo fenómeno, con el objetivo de: 1) establecer cuáles son los parámetros específicos que rigen la Política Criminal de la Unión Europea y analizar cada una de las medidas, de tipo normativo, operativo y preventivo, que conforman esta Política Criminal para definir si la misma posee o no una orientación punitiva al respecto hacia este delito; 2) enunciar los parámetros generales que rigen la Política Criminal de cada uno de los Estados escogidos y ejemplificar estas medidas, normativas, operativas y preventivas, en estos países que son objeto de caso de estudio, determinar su orientación hacia un modelo más o menos punitivo; 3) analizar las diferencias y similitudes de la Política Criminal de los Estados que representan los casos de estudio a fin describir el grado de armonización que posee cada uno respecto a la Política Criminal de la Unión Europea con relación al terrorismo yihadista en Internet.

Los tres Estados escogidos objeto de este estudio comparado son Alemania, Reino Unido y España. Estos tres países se tomarán como un caso de estudio, sobre los cuales se hará una revisión general de su Política Criminal a fin de determinar su aproximación a las medidas (normativas, operativas y preventivas) que implementa la Unión Europea.

Cabe mencionar que si bien Reino Unido, a tenor del Brexit¹, al presente no es un Estado Miembro de la Unión Europea, sí que lo era al momento de dar inicio a esta tesis doctoral. Por este motivo, aunado al hecho fundamental de que se hace ineludible su estudio debido a la historia compartida con los otros países mencionados por los hechos de terrorismo acontecidos en su territorio, se mantiene su análisis como Estado europeo geográficamente y políticamente vinculado a un problema común. Como nota adicional, es conveniente mencionar que tras el Brexit se establece en la Unión un nuevo orden a la coordinación europea en materia de seguridad y defensa, y específicamente en lo relativo al terrorismo. En lo referente a Reino Unido, cuyo estudio estará desarrollado en el capítulo 11 de esta tesis, su participación en Europa pasa de estar contenida en un convenio general² a ajustarse a lo pactado mediante acuerdos específicos de colaboración en este ámbito.

¹ Acrónimo de Britain (Gran Bretaña) y exit (salida). Se refiere a la salida de Reino Unido de la Unión Europea. Este proceso de salida se inició tras el referéndum convocado por Reino Unido hacia sus ciudadanos. Dicho referéndum fue celebrado el 23 de junio de 2016 y notificado al Consejo Europeo el 29 de marzo de 2017. Como consecuencia, el 31 de enero de 2020, Reino Unido salió oficialmente de la Unión Europea, y fue el 1 de enero de 2021 cuando, concluido el período transitorio estipulado para la retirada de Reino Unido de la Unión, dicha salida tuvo efectos plenos en los todos ámbitos sociales, políticos y económicos. El resultado del referéndum ha significado para Reino Unido la pérdida de su condición de Estado Miembro de la Unión Europea, y la adopción de la nueva consideración de Tercer Estado. Esto significa que ya no posee ninguna capacidad decisoria dentro de esta Organización Internacional. No obstante, esta retirada no implica la ruptura de relaciones presentes o futuras con la UE o sus instituciones, dado que Reino Unido continúa vinculado a la UE por medio de acuerdos de cooperación en diversas materias como, por ejemplo, aquellas que atañen a la seguridad de la región.

² Consejo de Europa, Convenio sobre la Ciberdelincuencia, Serie de Tratados N.º 185, de 23 de noviembre de 2001.

La delimitación temporal de este estudio se ciñe a los últimos 10 años, puntualmente al periodo comprendido entre 2013 y 2023, aunque no dejara por ello de mencionar documentos o normativa imprescindible en la materia; así como a hechos noticiosos relevantes, como el relativo al 11 de septiembre de 2001 en Estados Unidos de América (EE.UU.), cuyo atentado ha representado un hito internacional como punto de partida en la lucha contra el terrorismo en el mundo. Por el contrario, se afirma que el análisis de Internet con fines yihadistas estará delimitado a los últimos diez años, principalmente porque la profusión de contenido yihadista en la red es al presente tan extensa y veloz que, de no hacerlo, este estudio resultaría prácticamente inacabable.

En relación con los temas que quedan exentos de todo análisis en este compendio, es importante consignar de forma minuciosa que esta tesis doctoral no estudia todas las formas de terrorismo existentes, sino exclusivamente las de origen religioso y, dentro de estas, únicamente aquellas relacionadas con los grupos yihadistas. Tampoco estudia otras formas criminales que impliquen el uso de nuevas tecnologías, como el cibercrimen en general u otros tipos criminales en donde de cualquier forma estén vinculadas las herramientas informáticas.

No se estudia tampoco a la víctima del terrorismo, y no se estudia ni al terrorista ni a sus motivaciones y/o mentores. Por último, si bien se hace referencia directa en este estudio a los mismos por ser elementos constitutivos de opinión pública, no se estudia a los medios de comunicación ni a la sociedad, uno como grupo informativo y otro como grupo afectado respectivamente, de las acciones terroristas en los países citados.

En la estructura de este estudio doctoral titulado “La Política Criminal de la Unión Europea con relación al terrorismo yihadista en Internet”, se ha previsto diversos segmentos o unidades de análisis ordenadas por categorías temáticas.

Comienza con un preludio denominado *Planteamiento de la investigación* en donde se enuncian y describen todos los aspectos materiales y de forma relativos a esta tesis. Así, por ejemplo, encontramos en este segmento, la justificación que avala la necesidad de este estudio, los objetivos generales que persigue esta investigación y la descripción de la metodología utilizada para la recolección y el ordenamiento de los datos y la información.

Continúa con una *Introducción* temática del estudio en donde se enuncia brevemente la relevancia del fenómeno del terrorismo en Europa, el impacto de las nuevas tecnologías para el desarrollo del delito de terrorismo, la orientación de la Política Criminal de la Unión Europea y de los Estados analizados en relación con los crímenes de terrorismo online, conforme a las medidas de carácter normativo, operativo y preventivo, que han sido adoptadas. De igual forma, esta *Introducción* servirá para plantear las preguntas de investigación que regirán este estudio doctoral. Esta *Introducción* resulta en cierto modo en una antesala reflexiva y teórica de todo el estudio que se plantea a posteriori.

A continuación, se da apertura al segmento de las unidades específicas, y se inicia con la denominada *Parte I: Terrorismo y Terrorismo yihadista*. Esta parte, de contenido conceptual introductorio al tema, se encuentra dividida en tres capítulos: *Capítulo 1: El fenómeno del terrorismo internacional*, en donde se plantea una breve introducción sobre el terrorismo internacional y las características que lo definen, así también como el problema conceptual del término *terrorismo*. El *Capítulo 2: Internet como el espacio idóneo para una nueva oportunidad*

criminal, realiza un análisis de Internet como medio. Desde una perspectiva criminológica, se sugiere la idea de que Internet representa un nuevo medio de oportunidad criminal, y materializa el desplazamiento de un conflicto previo. Finalmente, en el *Capítulo 3: El uso yihadista de Internet y la e-yihad del autoproclamado Estado Islámico* se realiza una descripción de los usos habituales que realizan de Internet las organizaciones terroristas, atendiendo para ello a la clasificación de la United Nations Office on Drugs and Crime (UNODC); y se analiza el uso específico de la red por parte del autoproclamado Estado Islámico para el establecimiento y la profusión de su ideología.

La parte titulada *Parte II: La Política Criminal de la Unión Europea con relación al terrorismo yihadista en Internet*, aborda un análisis teórico de la Política Criminal y las medidas que se llevan a cabo dentro de la Unión Europea, y lo hace desde el capítulo 4 hasta el capítulo 7 inclusive. El primero de ellos, el *Capítulo 4: La Política Criminal de la UE ante el yihadismo online*, conceptualiza qué se entiende por Política Criminal, haciendo hincapié en los tres elementos que la componen, como son los instrumentos normativos, la gestión operativa e institucional y las medidas de prevención; y contextualiza la Política Criminal en el ámbito europeo haciendo hincapié en la búsqueda de seguridad común de la región. El *Capítulo 5: Medidas normativas europeas orientadas a la persecución del uso de Internet con fines yihadistas*, aborda completamente el primero de estos elementos constitutivos de la Política Criminal, describiendo en extenso la normativa internacional y europea vigente que permite dar alcance al yihadismo online. El *Capítulo 6: Medidas institucionales de la Unión Europea tendientes a la cooperación en el control y vigilancia de Internet y a la represión sobre su uso con fines yihadistas*, aborda el análisis de las acciones de contrterrorismo en este ámbito criminal específico, como la creación de centros especializados para la investigación de este fenómeno, la coordinación europea en el ámbito policial y judicial, el intercambio de información, el control de las fronteras exteriores de la Unión, etc., y lo plantea en tres niveles de acción, la cooperación entre instituciones y agencia de la UE con Estados Miembros, la cooperación entre Estados Miembros entre sí, y la cooperación entre la Unión Europea y socios estratégicos. Finalmente, en el denominado *Capítulo 7: Medidas preventivas y campañas de información y concienciación en la población europea*, se centra en el último instrumento de la Política Criminal de la Unión, analizando las campañas preventivas tendientes a evitar el reclutamiento y la radicalización en la región por medio de la creación de un contradiscurso en Internet. Describe también los programas de fomento a la educación y tolerancia religiosa, y diversas campañas de carácter informativo que se llevan a cabo en el marco de la Unión Europea y en sus Estados Miembros.

En la *Parte III: Revisión comparada de la Política Criminal de tres Estados europeos referente al uso de Internet con fines terroristas*, se aborda de forma individual el estudio de cada Estado en cuestión, es decir de Alemania, de Reino Unido y de España. Las revisiones individuales sobre cada Estado se realizan a través de la técnica metodológica de estudio de casos³. Estas revisiones generales se desarrollan entre los capítulos 8 y 10 inclusive, siendo el *Capítulo 8: Alemania*, el *Capítulo 9: Reino Unido*, y el *Capítulo 10: España*. En cada uno de estos capítulos se aplican los mismos criterios científicos utilizados para el previo análisis de la Unión Europea,

³ JIMÉNEZ CHAVES, Viviana Elizabeth/COMET WEILER, Cornelio (2016): «Los estudios de casos como enfoque metodológico», *ACADEMO Revista De Investigación En Ciencias Sociales Y Humanidades*, 3(2).

a saber, la revisión de las medidas normativas internas, de las medidas de control y vigilancia y represión adoptadas por cada Estado para la lucha contra el terrorismo en Internet conforme a su competencia y jurisdicción, y finalmente las medidas de desarrollo preventivo y diferentes campañas de información desarrolladas a nivel nacional. Al termino de cada capítulo se realizará una síntesis de la Política Criminal de cada Estado que nos permitirá una revisión comparada.

Finalmente, en las *Conclusiones y propuestas para fomentar la armonización de la Política Criminal en la Unión Europea en materia de terrorismo en Internet*, se procederá a enunciar las reflexiones y conclusiones a las que se han arribado en el marco de esta investigación. Se planteará a su vez propuestas que permitan desarrollar las orientaciones generales de la Política Criminal de la Unión. Esta última parte actúa como corolario de toda la tesis doctoral conforme representa, en términos constructivos, aquellas observaciones válidas de reseñar. De este modo, no solo se presentarán conclusiones del estudio, sino también ciertas premisas y pequeños puntos de partida para estudios futuros en esta materia.

JUSTIFICACIÓN

El terrorismo no supone un problema nuevo. Si se tienen en consideración los hechos documentados que a lo largo del tiempo han tenido lugar en muchas partes del globo, puede observarse que con asiduidad se ha utilizado la violencia para una finalidad política. Referirse en la actualidad al problema del terrorismo supone necesariamente incorporar un nuevo elemento de análisis: Internet. El uso de Internet por parte del terrorismo establece un nuevo suceso político que involucra no solo aspectos relativos a la persecución de este fenómeno, sino también a la aparición de nuevos factores de interés como la regulación de los proveedores de servicio, el desarrollo de nueva normativa, la consideración de nuevos tipos delictivos internacionales, el reconocimiento de la existencia o no de mentores para el desarrollo de este crimen, medidas de contra-terrorismo, el difícil equilibrio entre la persecución de este fenómeno y la protección de los derechos fundamentales, etc. Todo ello aunado a una nueva visión, establecida de forma conjunta y armonizada por los países de Europa en el marco de la UE.

Los usos que realizan de Internet los grupos terroristas⁴ se pueden condensar en dos grandes grupos claramente diferenciados: por un lado, se encuentra el uso con propósitos propagandísticos, enfocado en la difusión de sus atentados, motivaciones e ideología, y orientado a la captación, la incitación al terrorismo y la radicalización; y por otro lado, un uso basado en la acción operativa, y orientado a la coordinación estratégica de las propias acciones terroristas, como son la búsqueda de financiación, la planificación de atentados, e incluso la comisión de los mismos.

⁴ Autores como Gabriel Weimann y Miguel Ángel Cano Paños han desarrollado numerosos trabajos sobre el uso de Internet que realizan estas organizaciones o grupos terroristas. Weimann se pronuncia detalladamente sobre este fenómeno en diversos textos académicos, siendo en *Cyberterrorism*, su obra más referenciada, en donde cataloga los usos de Internet por parte de los grupos terroristas según este uso se implemente como medio o como fin. Cano Paños ha desarrollado ampliamente la aplicabilidad de este concepto en el análisis de ambos usos por parte del terrorismo yihadista, dando lugar a detallados casos de estudio sobre los usos de Internet que realiza el terrorismo en diversos países de Europa. A tenor de las “organizaciones o grupos terroristas” a los que se hace referencia, cabe señalar que se aplica la interpretación jurídica del concepto recogido en el art. 571 bis de la L.O. 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal español.

Entre las nuevas formas criminales que han surgido en la última década, puede considerarse al uso de Internet con fines terroristas como uno de los fenómenos transnacionales más relevantes, mediáticos y vigentes del presente. En la actualidad, el uso de Internet por parte del terrorismo yihadista es parte de la agenda de la gran mayoría de medios de comunicación europeos. Ello porque su uso por parte de estos grupos ha acrecentado aspectos relativos a la expansión de la propaganda terrorista, a la construcción de una ideología yihadista, y a una alta coordinación operativa a nivel global. Esto se ha traducido socialmente en una mayor visibilidad del terrorismo, fundamentalmente por el hecho de que los atentados o los escenarios de ataque por parte del yihadismo se consideraban circunscriptos a determinadas regiones del mundo. La visibilización del yihadismo en Europa y Estados Unidos ha establecido entonces, de facto, una nueva agenda política en materia de seguridad internacional, que no es indiferente ni a los medios de comunicación, ni a los ciudadanos.

La importancia que ha adquirido este delito en los últimos diez años ha sido determinante para que en Europa comenzaran a desarrollarse medidas orientadas a la erradicación y prevención del fenómeno. Las medidas adoptadas por la Unión son una evidencia de la lucha que libra la Unión Europea en esta materia. Desde una perspectiva normativa,

[...] «existen antecedentes que exponen la relevancia de este fenómeno. Desde la perspectiva legislativa nos podemos remontar al año 2008. Exactamente el 7 de abril de 2008 Europol publicó un informe en donde alertaba del uso creciente de Internet para difundir propaganda terrorista. A raíz de este informe el Parlamento Europeo dio su apoyo para la creación de una norma que obligara a tipificar como delito en todos los Estados Miembros conductas de inducción pública, captación y entrenamiento para el terrorismo a través de Internet.⁵ La norma fue aprobada en abril de 2008, si bien, previo a ello la Unión Europea ya contaba con una legislación marco en la materia⁶, aunque esta no cubría la difusión de propaganda.»⁷

Esta preocupación compartida por instituciones y Estados de la Unión ha creado un escenario global actual que redonda permanentemente en un mayor fomento de información científica en la búsqueda de soluciones.

La meta académica que persigue este texto parte de dos motivaciones específicas: la primera, el realizar aportes teóricos que se puedan traducir en toma de acciones tendientes al control de este tipo de crimen; y la segunda, contribuir a repensar el modelo de seguridad y los límites establecidos por los derechos humanos, de tal forma que en el control de estos crímenes no se atente colateralmente contra derechos fundamentales como la libertad de expresión o la libertad ideológica en Internet.

METODOLOGÍA

El tipo de investigación realizada para esta tesis doctoral es fundamentalmente de carácter descriptivo, y se enmarca en el ámbito de la ciencia criminológica.

⁵ Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo (DO L 330 de 9.12.2008).

⁶ Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (DO L 164 de 22.6.2002).

⁷ GADEA ALDAVE, Gilda (2014): «Delito y propaganda terrorista en Internet», en: RODRÍGUEZ TERCEÑO, José/FERNÁNDEZ PARADAS, Antonio (Coords.), *Nuevas culturas y sus lecturas*, Madrid: McGraw Hill, p. 255.

La metodología por emplear es mixta, dado que se realizará una investigación que integrará de forma sistemática métodos cuantitativos y cualitativos. Esta combinación de información nos permitirá tener una visión más completa del fenómeno a estudiar.

Al respecto Chaves-Montero sostiene que

«La investigación cuantitativa permite justificar la necesidad, descubre los problemas, los relaciona y los cuantifica. Por otra parte, la investigación cualitativa proporciona las bases para darle contenido, profundiza sobre las causas, caracteriza el funcionamiento y enriquece los cambios hipotéticos de solución. Finalmente podemos afirmar que la investigación mixta aumenta la posibilidad de ampliar las dimensiones en la investigación, y el sentido de entendimiento del fenómeno de estudio es mayor y más profundo.»⁸

Dentro de este esquema mixto de investigación se aplicarán cuatro instrumentos metodológicos, a saber: la revisión bibliográfica y documental, la revisión normativa, el análisis comparado y estudio de casos.

Esta tesis doctoral se focaliza en el análisis de la Política Criminal europea respecto al terrorismo yihadista en Internet. El planteamiento nos remite a la necesidad de estipular dentro del estudio un análisis teórico y conceptual que nos permita el entendimiento de la Política Criminal. Para ello se realiza una revisión bibliográfica en profundidad que faculta a crear un marco teórico adecuado al tema de estudio. Con la bibliografía indagada se pretenderá describir y definir que es la Política Criminal, como se construye, que elementos componen la misma, cuáles son los actores de ésta, cuál es su relevancia, etc. Para poder dar forma a este marco teórico se realizará la revisión bibliográfica de autores de referencia en el ámbito de la criminología, teniendo apoyo de fuentes bibliográficas provenientes del Derecho penal, y en menor medida aquellas provenientes de la sociología, ciencia política y relaciones internacionales. Esta última disciplina se tiene en cuenta a tenor de que el objeto de nuestro estudio es una organización supranacional, y que por ende la Política Criminal que se estudia no es la de un Estado, como habitualmente sucede, sino la de un organismo internacional.

En el desarrollo del estudio de la Política Criminal de Europa se analizarán también fuentes documentales y fuentes doctrinarias. La Unión Europea es una gran productora de documentos de toda índole. Habida cuenta de que se estudiará la Política Criminal de ésta, se analizarán informes, declaraciones, campañas informativas, campañas de prevención, contenido de páginas webs institucionales de la Unión, estrategias, protocolos, comunicados, etc. Esta revisión no solo se realizará en el ámbito europeo sino también ampliamente en el marco internacional, atendiendo a la dimensión global del fenómeno del terrorismo. Por ello se analizarán, entre otros, los documentos publicados por las Naciones Unidas, y organismos como la OTAN. Todo ello con la finalidad de conocer cómo operan las instituciones y agencias de la Unión Europea con relación al terrorismo en la red, y cuál es el marco de actuación policial, y de prevención que impera dentro de la Unión.

⁸ CHAVES-MONTERO, Alfonso (2018): «La utilización de una metodología mixta en investigación social», en: DELGADO SANTA GADEA, Kenneth/GADEA, Walter Federico/VERA-QUÍÑONEZ, Sara. (Coords.), *Rompiendo barreras en la investigación*, Machala: UTMACH, p. 165.

Con respecto a las fuentes doctrinarias, a fin de poder dar cuenta de uno de los elementos que componen la Política Criminal, se llevará a cabo un análisis jurídico mediante la revisión normativa del Derecho de la Unión en general y concretamente el Derecho penal de la Unión Europea, así como del Consejo de Europa. Se estudiarán por tanto decisiones de la Unión Europea, decisiones marco, reglamentos, leyes internas, etc. Se tendrán en cuenta a estos efectos también los tratados fundacionales de la Unión. En un marco externo a la UE, se revisarán resoluciones, tratados, convenios, etc. Se recurre, por tanto, a una amplia revisión normativa para conocer la respuesta jurídica frente a los delitos de terrorismo cometidos por medio del uso de Internet. Cabe destacar que, observando el ámbito jurisprudencial, se realizará también una revisión de sentencias con relación al uso de Internet con fines yihadistas dictadas en el marco de la Unión.

Finalmente, no debemos olvidar las fuentes bibliográficas y documentales que se analizarán sobre el terrorismo, el terrorismo yihadista, los fundamentos del islam, Internet, y las nuevas tecnologías. En este caso, parte de las fuentes documentales serán también obtenidas de los hechos noticiosos publicados en prensa virtual y física de medios de comunicación de reconocido prestigio, así como de centros de investigación europeos e internacionales, públicos y privados.

En concreto, la revisión bibliográfica y documental, se utilizará para la creación de todo un marco teórico apropiado para esta investigación. Será un gran punto de apoyo para establecer la perspectiva doctrinaria, y para la definición y delimitación de conceptos propios de la criminología. Para la realización de este constructo teórico, se considerarán las aportaciones de teóricos y autores de amplia trayectoria en el conocimiento de la criminología como ciencia autónoma. De igual forma, se realizará una amplia revisión bibliográfica sobre los aportes a la literatura científica de aquellos analistas de relevancia que centran su estudio disciplinar en Internet, en el terrorismo, en el delito de terrorismo cometido por medio de Internet, y en estudios disciplinarios *ad hoc* a nuestra investigación.

Por último, para la revisión de la Política Criminal de Alemania, Reino Unido y España, se utilizará como instrumento metodológico el análisis comparado y el estudio de caso. Este análisis comparado se desarrollará en torno a una línea sistematizadora, tendiendo a la segmentación y clasificación de las diversas unidades de análisis que componen este estudio. La unidad de análisis en concreto que será objeto de este instrumento metodológico será la Política Criminal de cada país referenciado. El instrumento metodológico de estudio de caso se empleará a fin de delimitar este segmento del estudio, restringiendo el análisis a un mero ejemplo ilustrativo y comparado dentro de la Política Criminal europea con respecto al terrorismo yihadista. Por tanto, no será un análisis en profundidad, sino tres casos de estudio que permitirán un abordaje comprado y ejemplificativo de la aplicación de la Política Criminal de la Unión Europea dentro de sus EEMM.

INTRODUCCIÓN

La Unión Europea es una Organización Internacional que posee una filosofía política orientada permanentemente hacia una estrecha unión de sus Estados Miembros, que es evidenciada por una integración cada vez mayor de un gran número de materias que la componen.

De entre todas estas materias sobre las cuales busca establecer un criterio común, aquella que es concerniente a la seguridad y a la defensa de la Unión resultó ser de las primeras que se han desarrollado activamente. La importancia que se le ha otorgado de forma temprana a la seguridad y defensa de la Unión ha ido perfilando la Política Criminal de esta, y ha permitido que la Unión Europea defina claramente sus prioridades y elabore las medidas necesarias para cumplir con sus objetivos en este ámbito.

La Política Criminal de la Unión Europea se encuentra enfocada en ámbitos delictivos de especial gravedad con dimensión transfronteriza.⁹ Dentro de estos delitos, la UE centra su especial atención sobre el delito de terrorismo. El terrorismo en Europa posee un largo recorrido, y ha tenido diversas fundamentaciones ideológicas a lo largo de su comisión. Desde una perspectiva historicista y académica podemos situar los inicios del terrorismo en Europa en el atentado al Parlamento inglés en torno al año 1600¹⁰. Posteriormente a este hecho, con el surgimiento del Estado moderno, nace un tipo de terrorismo, concretamente en Francia en el S. XIX, que dio inicio a lo que se conoce en la actualidad como terrorismo de Estado.

No obstante, a estos dos sucesos históricos, la noción del terrorismo moderno como lo conocemos en nuestro presente, que no requiere de información contextual para explicar el fenómeno, que se basta a sí mismo para ser entendido y que fundamenta gran parte de los estudios actuales, nace asociado a grupos no gubernamentales de pensamiento nacionalista.¹¹ La aparición en Europa de estos grupos políticos radicales, en el transcurso del S. XX, estableció en la región diversas formas de atentados y propaganda violenta que, por un lado, sembraron pánico y terror en la población europea, y por el otro dinamizó las diversas estructuras de los gobiernos nacionales para luchar contra este fenómeno extremista. De esta forma, los diferentes Estados del continente europeo desarrollaron una praxis propia, producto de su realidad política,

⁹ La delincuencia organizada, el terrorismo, la trata de seres humanos, la explotación sexual de mujeres y niños, los delitos PIF (Son aquellos que tienen un impacto negativo en el dinero de los contribuyentes de la UE, como fraude, corrupción, blanqueo de capitales y malversación). En la actualidad también se incluyen dentro de esta lista los delitos de especial gravedad con dimensión transfronteriza a los delitos de incitación al odio y los delitos motivados por el odio dentro de la UE. Véase: COMISIÓN EUROPEA (2021): *Comunicado de Prensa. La Comisión propone ampliar la lista de «delitos de la UE» a la incitación al odio y a los delitos motivados por el odio*, 9 de diciembre de 2021. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_21_6561 [Fecha de consulta: 09 de noviembre de 2023].

¹⁰ Conocido como la “Conspiración de la Pólvora”, se refiere al atentado previsto (frustrado) para el 5 de noviembre de 1605, donde rebeldes procatólicos intentaron hacer volar el palacio de Westminster (parlamento inglés) y matar al rey Jaime I de Inglaterra y a un gran número de parlamentarios, lores y jueces de la época.

¹¹ Nos referimos especialmente a la Hermandad Republicana Irlandesa (IRB), grupo nacionalista revolucionario con presencia en Irlanda y Estados Unidos de América; a Euskadi Ta Askatasuna (ETA), la organización terrorista nacionalista vasca con presencia en toda España; al Ejército Republicano Irlandés (IRA), el movimiento nacionalista cuyo objetivo era crear un Estado irlandés; la Fracción del Ejército Rojo (RAF), un grupo de izquierda de Alemania Occidental inspirado en Che Guevara, el socialismo maoísta y el Vietcong; y, las Brigadas Rojas, un grupo revolucionario de la izquierda italiana cuya pretensión era establecer un estado revolucionario por medio del uso de la violencia y la militarización.

que les permitió contribuir a una historia en común orientada a la lucha contra estas formas de violencia.

El terrorismo de origen islamista irrumpe con fuerza en el siglo XXI, concretamente el 11 de septiembre de 2001. Sí bien los atentados del 11-S tuvieron lugar en Estados Unidos de América, para todo el Sistema internacional resultó un hecho de extrema relevancia porque se estaba por vez primera frente a un tipo de terrorismo internacional que hizo sentir sus efectos en todo el mundo. En Europa, la materialización de este tipo de terrorismo no tardaría en llegar con una serie de atentados cuya autoría sería reconocida por las propias organizaciones yihadistas. Sí bien el primer atentado de origen islamista del que se tiene registro en España data de 1985¹², es recién a partir de los atentados en Madrid, en el año 2004¹³, cuando comenzaron una serie de atentados en Europa de similares características técnicas e idéntico fundamento ideológico. El atentado de Atocha sería entonces para Europa el puntapié inicial en la lucha contra el terrorismo yihadista.

La experiencia europea compartida hasta la fecha en la esfera del terrorismo había orientado de forma temprana a la Unión Europea a desarrollar normativa y medidas institucionales tendientes a la erradicación del terrorismo en la región, pero, aún con toda su andadura en esta materia, será recién con el fenómeno del terrorismo yihadista cuando la Unión Europea impulse los mayores avances para luchar contra esta modalidad de crimen. Y bajo la premisa de erradicación de este fenómeno se realizarán todo tipo de acciones normativas, institucionales y preventivas por parte de las instituciones y agencias de la Unión, así también como por parte de sus Estados Miembros.

Años más tarde, la incursión por parte del terrorismo yihadista en el uso de Internet para el desarrollo y ejecución de sus acciones delictivas significó una nueva materia de análisis dentro de la UE, y una actualización de su trabajo previo, en el ámbito legislativo, institucional y preventivo.

Teniendo en cuenta el devenir de este tipo de terrorismo en la región, podemos afirmar a priori que la propia Política Criminal de la Unión se ha ido desarrollando conforme el terrorismo evolucionaba hacia prácticas criminales más sofisticadas.

Hoy en día el terrorismo yihadista se orienta hacia el cibercrimen y el bioterrorismo. Sí bien aún no hemos entrado en ese periodo histórico en cual poder contabilizar atentados cometidos bajo estas modalidades, los diferentes investigadores y expertos de la Unión analizan el escenario actual y coinciden al brindar una prospectiva en la materia, afirmando que las citadas serán las futuras orientaciones delictivas del terrorismo yihadista.

Habida cuenta de esta nueva información, la Unión trabaja de forma temprana anticipándose a los acontecimientos criminales. Las medidas actuales llevadas adelante por la Unión Europea en la lucha contra el terrorismo yihadista en Internet sugieren que la Política Criminal de la

¹² El 12 de abril de 1985, tuvo lugar el atentado del restaurante El Descanso, situado en el kilómetro 14,200 de la carretera Madrid-Barcelona. En este atentado murieron 18 personas, todas españolas, y 85 resultaron heridas. Una llamada telefónica anónima a una agencia de noticias en Beirut afirmaba “*Reclamamos la responsabilidad de la operación que ha sido llevada a cabo en Madrid. Ha sido efectuada por el grupo de la mártir Abu Zeinab.*” A la fecha continúa sin resolver.

¹³ Los atentados del 11 de marzo de 2004 (11-M) fueron diez explosiones simultáneas en cuatro trenes de la red de Cercanías de la Comunidad de Madrid. Es conocido popularmente como “el atentado de Atocha” ha pasado a la historia como el mayor atentado cometido en España y el segundo mayor en Europa.

Unión está teniendo una vertiente anticipatoria del crimen y lo hace, siempre en un marco de respeto a los derechos fundamentales, mediante la investigación y la aplicación de la ley respecto a los usos de Internet con finalidad terrorista, mediante la colaboración entre instituciones, agencias y Estados de la UE, y mediante la prevención a fin de evitar las captaciones de nuevos miembros que quieran integrar las organizaciones yihadistas.

Para dar cuenta de todo lo expresado, a lo largo de toda esta tesis doctoral consideraremos la evidencia proporcionada por tres elementos fundamentales en la construcción de toda Política Criminal de un Estado¹⁴: la normativa existente en la materia delictiva, el marco institucional que permite la represión del crimen, y las medidas preventivas desarrolladas por la Unión o los Estados Miembros de la Unión.

Analizaremos, por tanto, cómo se ha consolidado el Derecho de la Unión Europea con relación al delito de terrorismo y de manera específica al delito de terrorismo en Internet. Estudiaremos la cooperación vertical y horizontal que tiene lugar entre las instituciones y agencias de la Unión Europea que intervienen en el proceso de lucha contra el terrorismo, entre las instituciones y agencias con los Estados Miembros, entre los Estados Miembros entre sí, y entre instituciones, agencias y EEMM de la Unión Europea con socios de terceros Estados y con empresas de tecnología de Internet. Y, finalmente, se estudiarán las campañas de carácter preventivo y de contradiscurso desarrolladas por la Unión Europea y por los Estados de la Unión, dirigidas a evitar el reclutamiento de nuevos miembros, así también como a reducir el impacto del radicalismo en miembros consolidados.

La Política Criminal de la Unión Europea, en la última década, se ha focalizado en los delitos de terrorismo. Ello es así no solo porque ha representado un crimen que ha tenido lugar en diversos Estados de la Unión, sino fundamentalmente porque, para la Unión Europea, el delito de terrorismo cumple con tres requisitos que lo encumbran como un crimen de especial importancia para la Unión. Podemos identificar tres categorías parcialmente superpuestas de crímenes europeos de especial importancia para la Unión: aquellos que atentan contra los intereses de la UE, más que contra los de los Estados Miembros individuales; aquellos que tengan un carácter claramente transfronterizo; y aquellos que destacan principalmente por su notoriedad pública. El cumplimiento de estas tres categorías permitiría encuadrar a un crimen dentro de los denominados crímenes de la Unión Europea, o eurocrímenes.

En términos generales, cuando nos referimos a crímenes se suele pensar en los mismos como delitos definidos por una norma, en donde el delito es un acto u omisión antijurídica que es sancionado por las leyes penales

Cuando hablamos de eurocrímenes, no podemos definirlos exclusivamente con referencia a la legislación de la UE. Sí bien el delito de terrorismo en Internet cumple sobradamente los criterios de cada categoría mencionada previamente, no posee la Unión Europea un Derecho penal común que pueda perseguir este delito. Debido a ello, los instrumentos de la UE son los que deben crear las reglas mínimas que los Estados Miembros deban y puedan implementar en sus legislaciones internas. Estas reglas son precisamente las que definen la Política Criminal de la Unión Europea frente al terrorismo. La Política Criminal de la UE no está solo basada en las normas del Derecho Europeo que la Unión utiliza como orientaciones para luchar contra este

¹⁴ En este caso, naturalmente, de una Organización Internacional.

crimen, sino que primordialmente se sustenta en la forma en la que la Unión Europea se enfrenta a este delito.

Un marco legal común que tiende a la armonización de las legislaciones internas de sus Estados Miembros, un sistema institucional que fomenta la cooperación horizontal y vertical entre sus instituciones, agencias y Estados, y un modelo preventivo que reivindica la importancia de la alerta temprana son los principales elementos de la Política Criminal de la Unión frente a este crimen. Este conjunto de medidas no para de crecer y siempre promueve la persecución de terrorismo yihadista online dentro de la Unión, a la vez que reivindican el Estado de Derecho y la prevalencia del sistema democrático.

La importancia del Estado de Derecho para una estrategia antiterrorista eficaz es ampliamente aceptada por gobiernos, expertos y ciudadanos de la Unión. La adhesión a los valores del Estado de Derecho protege tanto la legitimidad como la autoridad moral de las políticas y leyes antiterroristas.

PARTE I: TERRORISMO Y TERRORISMO YIHADISTA

CAPÍTULO 1: EL FENÓMENO DEL TERRORISMO INTERNACIONAL

Antes de adentrarnos específicamente en el terrorismo yihadista online resulta apropiado realizar una referencia al terrorismo internacional, dado que la existencia del primero deriva de un mejoramiento en la eficacia del segundo. Por tanto, no es posible hablar de terrorismo en Internet sin remitirnos obligatoriamente a su aspecto global. Esta característica no es un elemento *per se* del terrorismo, sino que fue construida de forma estratégica y en un tiempo determinado, y ha significado el primer paso evolutivo de este fenómeno.

Hace más de dos décadas tuvo lugar un cambio de paradigma en el mundo en torno a la seguridad internacional, ello debido principalmente al surgimiento de nuevas amenazas en este ámbito, que obligaron a los Estados y a las Organizaciones Internacionales a repensar la seguridad y la propia defensa. No cabe ninguna duda de que el punto de partida y el epicentro en el calendario de esa nueva era se fijó el 11 de septiembre de 2001. El caso de las Torres Gemelas en Nueva York no solo supuso la desestabilización política y un gran impacto en la opinión pública de Estados Unidos de América, sino también de todo el Sistema internacional. Con este hecho se abría la puerta a un nuevo terrorismo de tipo transnacional que podía (y quería) hacer sentir sus efectos más allá de cualquier frontera. Como publicaría en su portada el periódico *El Economista*¹⁵, el 11 de septiembre de 2001 fue “el día que el mundo cambió”.¹⁶ Mas allá del acierto editorial de entonces, se desconocía por aquella época que el terrorismo local (propio del terrorismo de guerrilla en Latinoamérica, o de organizaciones con intereses regionales como las derivadas de las reivindicaciones violentas de ETA o IRA, en España e Irlanda del Norte, respectivamente), pasaría paulatinamente y con los años a un segundo plano de amenaza, en cuanto se le observaría circunscripto a un territorio de acción autodelimitado. Ello primordialmente porque este “viejo”¹⁷ o tradicional terrorismo local, al no expandir geográficamente sus acciones, no sería visto como una amenaza para el Sistema internacional.

¹⁵ «The day the world changed», *The Economist*, edición online de 13 de Septiembre de 2001. Disponible en: <https://www.economist.com/leaders/2001/09/13/the-day-the-world-changed> [Fecha de consulta: 13 de noviembre de 2013].

¹⁶ Los atentados del 11 de septiembre de 2001, conocidos bajo el acrónimo 11S en España y 9/11 en el mundo anglosajón así como en países de Latinoamérica, fueron una serie de atentados terroristas en modalidad suicida y de gran magnitud contra centros neurálgicos y emblemáticos del poder político y económico de Estados Unidos de América.

Estos atentados fueron perpetrados en un mismo día y con una mínima temporalidad entre uno y otro, por medio de ataques suicidas en los cuales terroristas tomaron el control de cuatro aviones comerciales mientras sobrevolaban territorio estadounidense con el objetivo de hacerlos estallar contra cuatro destinos estratégicos de esta nación. El primer ataque tuvo lugar a las 8:46 a.m. del 11 de septiembre de 2001, e implicó el secuestro del Vuelo 11 de American Airlines (AA) y su posterior impacto contra la torre norte del World Trade Center (WTC). El segundo ataque tuvo lugar a las 9:03 a.m. cuando el vuelo 175 de United Airlines (UA) impactó contra la torre sur del mismo objetivo. A las 9:37 hs de esa misma mañana, el vuelo 77 de AA colisiona contra la sede del Departamento de Defensa de los Estados Unidos, el Pentágono. Finalmente, a las 10:03 a.m. el cuarto avión secuestrado, el vuelo de 93 de UA que se dirigía a Washington D.C., se estrella en Pensilvania sin concretar su objetivo, por la actuación de pasajeros y tripulación que impidieron el atentado.

La autoría de dichos ataques se la autoadjudicó el grupo terrorista de origen islámico Al Qaeda mediante un video protagonizado por Osama Bin Laden, el líder de dicha organización e ideólogo del 11S.

Desde una perspectiva academicista, lo estrictamente relevante de estos atentados acontecidos hace más de 20 años es que han sido los primeros actos terroristas con modalidad transnacional y son a su vez los que han convirtieron al terrorismo en el actual fenómeno yihadista global.

¹⁷ CANO PAÑOS, Miguel Ángel (2010b): «Reflexiones en torno al “viejo” y al “nuevo” terrorismo», *Revista Española de Investigación Criminológica (REIC)*, Artículo 7, Número 7, pp. 21-56.

Otra de las consecuencias de los ataques de 2001 en Estados Unidos, y que ha pasado a constituir uno de los principales elementos por medio del cual se define al terrorismo internacional, deriva de la respuesta reactiva de los gobiernos nacionales que comenzaron a profundizar en el desarrollo de esfuerzos comunes para combatir esta modalidad de crimen. Así, desde la fecha señalada hasta el día de hoy, se han creado en todo el mundo numerosas unidades de inteligencia que trabajan intergubernamentalmente, y de forma coordinada en la lucha contra el terrorismo, en operaciones conjuntas o en el intercambio de información.

Estas organizaciones y agencias de inteligencia estatales, con el objeto de investigar estos crímenes en el ámbito interno y externo, se han dado a la tarea de definir qué entienden por terrorismo. De esta forma, aun cuando al presente no existe una definición consensuada que facilite la labor de los operadores jurídicos, puede recurrirse a diversas aproximaciones de índole institucional que facilitan la contextualización y persecución de este crimen.

Por ejemplo, el FBI define terrorismo como una actividad que implica el uso ilegítimo de la fuerza en contra de personas o propiedades con fines de intimidación o coerción a un gobierno, población civil (o un segmento de ella) en la consecución de objetivos políticos o sociales¹⁸, mientras que en el ámbito académico la definición de terrorismo posee mayores matizaciones a fin de reducir al máximo el uso discrecional del término por parte de los Estados. Cabe señalar que solamente en Estados Unidos son aplicables tres definiciones legales distintas sobre el delito de terrorismo, la del Código Penal, la del FBI y la del Departamento de Defensa.¹⁹ El problema conceptual en torno a la definición de terrorismo se acentúa si tenemos en cuenta más legislaciones como es el caso de la Unión Europea. Por este motivo, antes de adentrarnos en el objeto principal de este estudio, nos será de utilidad delimitar conceptualmente la información referida al terrorismo y el terrorismo internacional.

Es necesario comenzar por el hecho de que en el presente no existe una definición universal de lo que se entiende por terrorismo.²⁰ No obstante existen claras nociones construidas a través de referencias en diversas declaraciones universales, protocolos, convenciones y sentencias. Si bien no se ha alcanzado hasta la fecha un consenso respecto a la definición de terrorismo, pueden encontrarse tempranamente indicios de búsqueda de esta uniformidad.

En 1937, la Sociedad de Naciones enunció en la Convención para la Prevención y la Represión del Terrorismo²¹ que se estaba frente a un acto de terrorismo cuando se perpetraran “actos

¹⁸ WHITTAKER, David. J. (2003): *The Terrorism Reader*, London: Routledge.

¹⁹ Definición del Código Penal: 'Violencia premeditada y políticamente motivada contra objetivos no combatientes, cometida por grupos infranacionales o actores clandestinos, habitualmente pensados para influir a un público'. Definición del FBI: 'Uso ilegítimo de la fuerza o la violencia contra personas o propiedades para intimidar y coaccionar a un Gobierno, a una población civil o a cualquier segmento de ésta, para la consecución de objetivos políticos o sociales'. Definición del Departamento de Defensa: 'Uso ilegítimo, o amenaza de la fuerza o violencia contra individuos o propiedades para coaccionar o intimidar a los Gobiernos y a las sociedades, a menudo para obtener objetivos políticos, religiosos o ideológicos'.

²⁰ La falta de consenso se debe principalmente al hecho de que los Estados son reticentes a tipificar como actos de terrorismo los crímenes perpetrados por ellos mismos.

²¹ La Convención para la Prevención y la Represión del Terrorismo se adoptó el 16 de noviembre de 1937, tras la firma de 24 Estados. En ella se detallaban las acciones denominadas antiestatales, tales como ataques a funcionarios públicos, ataques a jefes de Estado, así como a sus familias y/o la destrucción de instalaciones públicas. Asimismo, exigía a los Estados signatarios la promulgación de leyes que facilitaran la extradición para este tipo de actos a fin de poder penar los actos de terrorismo de un ciudadano en un país extranjero. La convención nunca fue ratificada por tanto no entró en vigor, debido principalmente a desacuerdos en materia de extradición. El documento se conserva en los archivos propios de la Sociedad de Naciones. Los mismos han sido transferidos a las Naciones Unidas en 1946 y se encuentran en su oficina de Ginebra. Se inscribieron en el registro de Memoria del Mundo de la UNESCO en 2010.

criminales dirigidos contra un Estado, con la intención o el propósito de crear un estado de terror en la mente de un individuo, de un grupo de personas o del público en general.”

El 17 de diciembre de 1996 se adopta en la Asamblea Plenaria la resolución 51/210: “Medidas para eliminar el terrorismo internacional”. Este documento se aprueba el 16 de enero de 1997 y busca realzar la importancia que deben tener las Naciones Unidas y los organismos especializados competentes en la lucha contra el terrorismo internacional en una nueva etapa de mayores desafíos en cuanto al terrorismo internacional, dado que los ataques terroristas son cada vez más mortíferos y difundidos.

Se cita como precedente de cooperación la resolución 49/60, del 9 de diciembre de 1994, por la que se adoptó la Declaración sobre medidas para eliminar el Terrorismo Internacional, y la resolución 50/53, del 11 de diciembre de 1995. Se observa en este nuevo contexto la necesidad de implementar esfuerzos regionales e internacionales y se alienta a los Estados a examinar sus disposiciones jurídicas nacionales que contemplen la prevención, represión y eliminación del terrorismo internacional. Es importante destacar que por vez primera se alienta a considerar a futuro, la creación de una convención general sobre Terrorismo Internacional.

Una supuesta convención general aplicable a todo el Sistema internacional debería, como punto de partida, tener una definición uniforme de lo que es o que se entiende por terrorismo. La Oficina Contra la Droga y el Delito de las Naciones Unidas (UNODC) ha recogido desde muy tempranamente las nociones teóricas de Alex Schmid.²² Este autor considera que debe tomarse el concepto de crimen de guerra²³ como punto de partida.

Schmid y Jongman alegan que de hacerse extensiva su definición a un tiempo de paz, se puede establecer una razonable analogía afirmando que los actos de terrorismo son los equivalentes, en tiempo de paz, a los crímenes de guerra.²⁴ De esta forma, Schmid y Jongman dan paso a una primera definición que será recogida por las Naciones Unidas en su interpretación del terrorismo.

Para estos autores,

[...] «el terrorismo es un método de acción violenta repetida que inspira ansiedad, utilizado por actores clandestinos individuales, colectivos o estatales semiclandestinos, por razones de idiosincrasia, de orden criminal o políticas, según el cual los blancos directos de la violencia no son los blancos principales. Las víctimas [...] de la violencia son escogidas generalmente al azar (blancos de oportunidad) o de forma selectiva (blancos representativos o simbólicos) [...] y sirven para generar un mensaje. Los procesos de comunicación basados en la violencia o en la amenaza [...] son utilizados para manipular el blanco principal (el público objetivo) haciendo de éste un blanco del terror, un blanco de las exigencias o un blanco de atención, según el principal objetivo sea la intimidación, la coerción o la propaganda.»²⁵

²² Uno de los primeros teóricos en intentar consensuar una definición de terrorismo. Véase: SCHMID, Alex P. (2004): «Estadísticas sobre el terrorismo: Dificultades de medir las tendencias del terrorismo mundial», en: SCHMID, Alex P. (Ed.), *Foro sobre el delito y la sociedad*, Vol. 4, N.º 1 y 2, New York: UNODC, pp. 55-78.

²³ El art. 8 del Estatuto de Roma de la Corte Penal Internacional establece la competencia de la Corte y la tipificación de los delitos que la integran.

²⁴ JEFFREY, Ian Ross (2006): *Political Terrorism: An Interdisciplinary Approach*, New York: Peter Lang Publishing, p. 7.

²⁵ SCHMID, Alex. P./JONGMAN, Albert. J. (2005); *Political Terrorism: A new guide to actors. Authors, concepts, data bases, theories, and literature*, New Brunswick: Transaction Publishers, p. 28. Cita original: “*Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target*

Ateniéndose al ámbito de organización regional, es relevante mencionar que la Organización de Estados Americanos aprobó el 3 de junio de 2002 la Convención Interamericana contra el Terrorismo²⁶. Esta Convención, en vigor desde el 7 de octubre de 2003, promueve la obligación de sancionar leyes de protección contra el terrorismo en todos los Estados americanos, con el objeto de establecer un sistema continental de represión contra el terrorismo.²⁷

La Convención Interamericana contra el Terrorismo enfatiza en su artículo 4 en la necesidad de establecer medidas jurídicas y administrativas para combatir el terrorismo sin afectar los derechos humanos (art. 15) haciendo hincapié en que los Estados parte “propiciarán una amplia cooperación”²⁸ (art. 17) para combatir el terrorismo.

Entre los importantes inconvenientes que presenta el Convenio es destacable el hecho de que con independencia de la voluntad de las partes, resulta imposible alcanzar una definición de terrorismo en el documento, así también como alcanzar un consenso para calificar el terrorismo como crimen de lesa humanidad.

Considerando el marco internacional es importante detallar que, en un informe de la Naciones Unidas²⁹ del 2 de diciembre de 2004 realizado por el Grupo de Alto Nivel sobre las Amenazas, los Desafíos y el Cambio³⁰ se reconoce el problema normativo derivado de la carencia de una definición de terrorismo. En él se reconoce que la capacidad de las Naciones Unidas para elaborar una estrategia amplia se ha visto limitada por el hecho de que los Estados Miembros no han podido aprobar un convenio sobre el terrorismo que incluya una definición del terrorismo. Según las Naciones Unidas, “la búsqueda de un acuerdo sobre la definición del terrorismo se topa generalmente con dos obstáculos. El primero es el argumento de que cualquier definición debe incluir el caso de un Estado que use fuerzas armadas contra civiles. Consideramos que el marco jurídico y normativo aplicable a las violaciones por parte de los Estados es mucho más sólido que en el caso de los actores no estatales y no creemos que esa objeción sea convincente. La segunda objeción es que un pueblo bajo ocupación extranjera tiene derecho a resistirse y que una definición del terrorismo no debería derogar ese derecho. El derecho a resistirse es cuestionado por algunos. Pero el quid de la cuestión no es ese, sino el hecho de que la ocupación de ninguna manera justifica el asesinato de civiles.”³¹

population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperial) victims and main targets are used to manipulate the main target (audience[s]), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.”

²⁶ Convención Interamericana contra el Terrorismo, AG/RES. 1840 (XXXII-O/02), aprobada en la primera sesión plenaria celebrada el 3 de junio de 2002.

²⁷ Busca eliminar limitaciones para actuar tales como, el secreto bancario, la invocación de delito político, la condición de refugiado o el derecho de asilo.

²⁸ Cooperación entre Estados Miembros y entre los órganos de la Organización de Estados Americanos, incluido el Comité Interamericano contra el Terrorismo (CICTE). Debe tenerse en cuenta la resolución RC.23/RES.1/01 rev. 1 corr. 1 “Fortalecimiento de la cooperación hemisférica para prevenir, combatir y eliminar el terrorismo” de la Vigésima Tercera Reunión de Consulta de los Ministros de Relaciones Exteriores del 21 de septiembre del 2001, que encomendó al Consejo Permanente la elaboración de un Proyecto de Convención Interamericana contra el Terrorismo.

²⁹ Véase UN. Doc. A/59/565, de 2 de diciembre de 2004.

³⁰ El Grupo de Alto Nivel fue creado en diciembre de 2003 a petición del Secretario General de las Naciones Unidas, para evaluar las actuales amenazas a la paz y la seguridad internacional con el objeto de formular recomendaciones para fortalecer las Naciones Unidas con el fin de proporcionar seguridad colectiva en el siglo XXI. Formado por 16 expertos independientes, compuesto por miembros con representación geográfica equitativa y un miembro por cada Estado Miembro del Consejo de Seguridad. Véase UN Doc. A/58/612, de 28 de noviembre de 2003.

³¹ UN. Doc. A/59/565, de 2 de diciembre de 2004; p. 53.

En vista de que la Asamblea General posee legitimidad en lo referido a cuestiones normativas, y a fin de instar a la necesidad de arribar a un consenso de la definición de terrorismo, propone una definición de terrorismo en el seno de la Asamblea General.

Esa definición del terrorismo debería incluir los elementos siguientes:

- a) El reconocimiento en el preámbulo de que el uso de la fuerza contra civiles por parte de un Estado está sujeto a las disposiciones de los Convenios de Ginebra y a otros instrumentos y que, en escala suficiente, constituye un crimen de guerra o de lesa humanidad;
- b) La reiteración de que los actos comprendidos en los 12 convenios y convenciones anteriores contra el terrorismo constituyen actos de terrorismo y una declaración de que constituyen un delito con arreglo al derecho internacional y la reiteración de que los Convenios y Protocolos de Ginebra prohíben el terrorismo en tiempo de conflicto armado;
- c) Una referencia a las definiciones contenidas en el Convenio internacional de 1999 para la represión de la financiación del terrorismo y la resolución 1566 (2004) del Consejo de Seguridad;
- d) La siguiente descripción del terrorismo:

«Cualquier acto, además de los actos ya especificados en los convenios y convenciones vigentes sobre determinados aspectos del terrorismo, los Convenios de Ginebra y la resolución 1566 (2004) del Consejo de Seguridad, destinado a causar la muerte o lesiones corporales graves a un civil o a un no combatiente, cuando el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo.»³²

El Grupo de Alto Nivel confía en que la existencia de una definición de terrorismo en la Naciones Unidas promueva la creación de un convenio general relativo a terrorismo.

En el punto número 11 de las Conclusiones y Recomendaciones del documento A/59/565, en una Nota perteneciente al Secretario General, se menciona la conclusión de que en la lucha contra el terrorismo las Naciones Unidas no han aprovechado de manera óptima los recursos de los que disponen.

Como afirma con razón el Grupo, las Naciones Unidas deben poder “articular una estrategia contra el terrorismo eficaz y basada en principios, que respete el Estado de Derecho y la observancia universal de los derechos humanos. Uno de los obstáculos que hasta la fecha se han opuesto a ello es, en mi opinión, la incapacidad de los Estados Miembros de llegar a un acuerdo sobre una definición del terrorismo. El informe ofrece una definición de terrorismo, y en el mismo se pronuncia el Secretario General de las Naciones Unidas expresando que está

³² *Ibidem*; p. 54.

convencido que “ello ayudará a formar el consenso que necesitamos para avanzar rápidamente en el sentido derecho”.³³

Para Schmid, el terrorismo es un complejo fenómeno multidimensional que hace que el termino de terrorismo sea usado de forma irrestricta para una gran variedad de manifestaciones (como, por ejemplo, narcoterrorismo, ciberterrorismo, etc.) de tal forma que uno termina preguntándose si existe un único concepto de terrorismo. Este uso masivo en múltiples contextos ha hecho que el termino carezca de significado.³⁴

En el año 2004, en el marco de un estudio titulado *The Challenges of Conceptualizing Terrorism*, realizado por Weinberg, Pedahzur y Hirsch-Hoefler, se analizaron 73 definiciones de terrorismo extraídas de cuatro revistas especializadas en terrorismo. Esto permitió consensuar algunos aspectos repetitivos que se han tomado como parte de denominadores comunes para una definición. A saber: “El terrorismo es una (1) táctica con (2) motivaciones políticas que implica la (3) amenaza o el uso de fuerza o (4) violencia en el que la búsqueda de la (5) publicidad desempeña un papel significativo”.³⁵

Según Schmid³⁶ el problema que presenta la definición de Weinberg, Pedahzur y Hirsch-Hoefler es que simplifica al extremo la conceptualización, permitiendo que sea una definición muy general. Así, por ejemplo, la definición de Weinberg [et. al.] no hace referencia alguna a las víctimas o perpetradores, no menciona la idea de miedo o terror, engloba todas las motivaciones bajo una idea política y no menciona el aspecto criminal o inmoral de la naturaleza de las tácticas (secuestro, toma de rehenes, asesinato indiscriminado, asesinatos sectorizados, etc.). Es decir, en la búsqueda del consenso de lo que es terrorismo se ha reducido a niveles mínimos su complejidad.

El concepto de miedo o terror, lo podemos encontrar con Reinares cuando afirma que “un acto de violencia es terrorista si el impacto psíquico que provoca en una sociedad o algún segmento de la misma, en términos de ansiedad y miedo, excede con creces sus consecuencias materiales”³⁷. Con ello se refiere al hecho de que la sensación de terror que provoca es mayor a los daños físicos ocasionados a personas o cosas.

Con relación a este aspecto, Calduch Cervera considera “esencial comprender que terrorismo es una estrategia de acción que busca provocar la ruptura del orden de convivencia social de los países, a través de la generación y propagación del terror como una manifestación emocional derivada de una percepción de inseguridad extrema.”³⁸

³³ Ibidem; p.3.

³⁴ SCHMID, Alex (2004): «Terrorism. The definitional problem», *Reserve Journal of International Law*, 36(2), pp. 375-420.

³⁵ Leonard Weinberg, Ami Pedahzur y Sivan Hirsch-Hoefler han establecido la *Academic Consensus Definition* (Definición académica consensuada). Véase: WEINBERG, Leonard/PEDAHZUR, Ami/HIRSCH-HOEFLER, Sivan (2004), «The Challenges of Conceptualizing Terrorism», *Terrorism and Political Violence*, 16(4), 777-794, p. 782.

³⁶ SCHMID, Alex (2004), opus cit., pp. 375-420.

³⁷ REINARES, Fernando (2005): «Conceptualizando el terrorismo internacional», *Análisis del Real Instituto Elcano*, (24), Madrid: Real Instituto Elcano, 4-7, p. 4.

³⁸ CALDUCH CERVERA, Rafael (2007): «Conflictos internacionales culturales y violencia terrorista», *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, 22-80, p. 63.

Un conflicto similar se presenta en el abordaje teórico de lo que se entiende por terrorismo internacional. Según Reinales, la existencia del terrorismo internacional comprende necesariamente dos aspectos; el primero es que las acciones terroristas se practiquen con la deliberada intención de afectar la estructura y distribución del poder en regiones enteras del planeta o incluso a escala misma de la sociedad mundial; y el segundo aspecto necesario para que el terrorismo sea considerado internacional, es que sus actores individuales y/o colectivos hayan extendido sus actividades por un significativo número de países o áreas geopolíticas, en consonancia con el alcance de los propósitos declarados.³⁹

El terrorismo internacional suele perpetrarse de manera sistemática e impredecible, “por lo común dirigido contra blancos dotados de alguna relevancia simbólica en sus correspondientes entornos culturales o marcos institucionales de referencia. Blancos a menudo de oportunidad, cuyo menoscabo o destrucción son utilizados para transmitir mensajes y dotar de credibilidad a eventuales amenazas proferidas, lo cual convierte al terrorismo en un método extremista tanto de propaganda como de control social.”⁴⁰

Es importante destacar que, con independencia de las limitaciones presentadas en términos conceptuales por la carencia de una definición de uso universal de Terrorismo, el Soft Law ha ido permitiendo la construcción del término y posibilitando el establecimiento de ciertas características propias del fenómeno. En este sentido, Abad Castelos afirma que, si bien no es imprescindible una definición consensuada de terrorismo dado que se ha ido operando respecto de este delito, sí resulta necesaria en cuanto que “las normas internacionales existentes descansan primordialmente en la actuación de los operadores jurídicos (judiciales o gubernamentales) internos” y es por tanto crucial “el carácter adecuado de las definiciones (y normas) internas” a fin de garantizar el principio de seguridad jurídica.⁴¹

En el terrorismo internacional no existe una sustancial diferencia respecto la interpretación del terrorismo descrita en estos últimos casos, excepto por el alcance de sus efectos. Es, por tanto, el carácter esencialmente global de estos ataques lo que resulta en la principal característica para definir el terrorismo internacional. Podríamos sintetizar sus características en la siguiente enumeración:

1. Implica una actividad planificada:

Por actividad planificada se entiende cualquier acción que haya sido planeada de forma estratégica bajo premisas que permitan la consecución de los objetivos previamente definidos. Implica el planteamiento y ejecución de actos violentos y no violentos (por ejemplo, actos preparatorios).⁴²

³⁹ REINALES, Fernando (2005), opus cit., pp. 4-7.

⁴⁰ *Ibidem*, p. 4.

⁴¹ Dado que “la calidad de las normas internas depende en gran medida de las normas internacionales”, Abad Castelos termina por percibir que se está frente a un círculo vicioso, cuya ruptura depende de la existencia de una definición internacional. Véase: ABAD CASTELOS, Monserrat (2012): «El concepto jurídico del terrorismo y los problemas relativos a su ausencia en el ámbito de las Naciones Unidas», en: CONDE PÉREZ, Elena (Dir.) / IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, p.114-115.

⁴² “[...] los terroristas planifican estratégicamente sus acciones.” Véase: GARCÍA GURRIONERO, Mario (2013): *El papel del terror en la sociedad*, Madrid: Maia, p. 35.

2. Puede ser perpetrada por un actor individual u organizacional:

La acción terrorista puede llevarla a cabo por un solo individuo (actor individual, o lobo solitario en el caso del terrorismo yihadista) o, por un grupo de individuos (actor organizacional u organización terrorista). En el primer caso el actor responde de forma solitaria a un modelo de ataque prefijado por la organización, pero no necesariamente responde a una directiva expresa de la misma. Puede tratarse de simpatizantes del grupo terrorista que se adhieren a su ideología y que de forma espontánea y voluntaria y solidaria actúan individualmente para los fines del conjunto. En el último caso, se está frente al accionar de un actor complejo que involucra la existencia de una estructura, aunque no necesariamente piramidal como en el caso del yihadismo.

3. Relación simbiótica con los medios de comunicación:

El terrorismo persigue entre otros fines específicos, la cobertura mediática. Planifica sus atentados a fin de ofrecer el mayor impacto visual posible. “El terrorismo es [...] un proceso de comunicación entre terroristas y audiencias”.⁴³ A diferencia de otro tipo de crímenes, el terrorismo entiende que parte de su eficacia está dada en la difusión de sus acciones. El terrorismo “persigue con sus acciones criminales una publicidad, una intención comunicativa que va más allá de su violencia política”.⁴⁴ Es por ello por lo que la relación con los medios es característica, dado que, por otra parte, los medios difunden profusamente imágenes de los atentados en la búsqueda de nuevas audiencias.

4. Violencia política hacia públicos directos e indirectos:

Las acciones del terrorismo se dirigen a un público indirecto, habitualmente sujetos individuales o institucionales tales como gobiernos, personas públicas, políticos, etc., y lo hacen a través de las acciones violentas que ejercen en la sociedad contra públicos directos.⁴⁵ Estas acciones buscan que los públicos indirectos cedan a las demandas del terrorismo.⁴⁶

“El yihadismo global ha aplicado varias líneas de actuación para alcanzar sus objetivos. Por supuesto, la primera y fundamental implica la planificación y ejecución de actos y campañas violentas.” Véase: DE LA CORTE IBÁÑEZ, Luis (2012): «El terrorismo yihadista internacional a principios del siglo XXI», en: CONDE PÉREZ, Elena (Dir.) /IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, p. 33.

⁴³ *Ibidem*; p. 30.

⁴⁴ “[...] a partir de los atentados del 11-S, el terrorismo entra en la escena comunicativa. Tal es el caso del terrorismo mediático o nueva era del terrorismo” [...] “Los terroristas son conscientes de que la violencia política es un potente medio para penetrar en los vínculos entre los medios de comunicación, el público en general y el gobierno, tanto a nivel nacional como internacional.” Véase: GARCÍA GURRIONERO, Mario (2013), *opus cit.*, p. 31-33.

“El terrorismo sabe que causa miedo, y el miedo siempre es noticia, puesto que la información aparenta calmar ese miedo y, por tanto, el conocimiento del porvenir debería crear una vía de escape para toda situación angustiosa. Pero se da la paradoja de que la información proporcionada por los medios muchas veces no despeja las dudas y, en consecuencia, no elimina el miedo, sino que lo potencia.” [...] “el terrorismo guarda una estrecha relación con los medios de comunicación y el peligro de esa estrecha relación, que medios de comunicación y terrorismo mantienen, es la certeza de que ese vínculo supone una especie de simbiosis, ya que, si bien los terroristas encuentran en los medios el eco deseado para propagar su denominación o su propio mensaje, los terroristas proporcionan, a su vez, el espectáculo que los periodistas necesitan para satisfacer a la audiencia.” Véase: VERES CORTÉS, Luis (2005): «La simbiosis del terrorismo con los medios de comunicación», en *Información para la paz: autocrítica de los medios y responsabilidad del público*. Actas del Congreso Internacional de Ética y Derecho de la Información organizado por la Universidad CEU Cardenal Herrera, pp. 587-594.

⁴⁵ REINARES, Fernando (2005), *opus cit.*, p. 4-5.

⁴⁶ Excepcionalmente se puede encontrar un caso contrario a esta realidad descripta: “Creo que dicha circunstancia sólo se ha dado en Italia con el grupo Autonomía Obrera en los años sesenta. Esta banda armada escogía sus víctimas, no entre personalidades de

5. Uso de la violencia o amenaza del uso de la violencia:
El terrorismo implica necesariamente el uso de la violencia. Ello resulta contrario al Estado de Derecho en cuanto rompe con el monopolio del uso legítimo de la violencia⁴⁷ por parte del Estado. El uso de la violencia revela el aspecto criminal del terrorismo en virtud que es el instrumento del cual el terrorismo se vale en la búsqueda de logros de sus objetivos políticos.⁴⁸
6. Deliberada intención de afectar la estructura y la distribución de poder en un Estado:
El terrorismo persigue una finalidad política conforme intenta subvertir el orden establecido en un Estado. Busca por medio de sus acciones violentas influir en el público indirecto con el objeto de que sus demandas políticas sean atendidas. Estas demandas se encuentran a menudo en estrecha oposición con la estructura de poder que es objeto del reclamo.⁴⁹
7. Poseen actividades en un número de países o áreas geopolíticas:
Debemos referirnos a terrorismo internacional cuando las acciones se desarrollen en más de un Estado o región geopolítica.⁵⁰ La presencia de este aspecto debe hacernos suponer que estamos frente a un grupo terrorista con presencia global o con pretensiones de expansión global, por lo que la cooperación internacional resulta determinante.
8. Autofinanciación:
El terrorismo obtiene sus ingresos por medio de las mismas acciones que la propia organización realiza y mediante la implicación en otras actividades delictivas, tales como narcotráfico, secuestro extorsivo, tráfico de armas, trata de personas, etc.⁵¹
9. Intención de infundir terror y de alterar la paz pública:

renombre, directivos, políticos, militares, empresarios, etc., sino entre cargos intermedios del mundo empresarial: capataces, directores de personal, etc. La razón era fácil de intuir. Autonomía Obrera rehuía de la publicidad para no evidenciar su estrategia contra el Estado y contra los que ellos consideraban sus principales enemigos, es decir, las empresas.” Véase: VERES CORTÉS, Luis (2005), opus cit., p. 594.

⁴⁷ WEBER, Max (1967): *El político y el científico*, Madrid: Alianza.

⁴⁸ “Asimismo, los incidentes terroristas vinculados al yihadismo global han destacado por su carácter generalmente indiscriminado, por una letalidad muy superior a la de otros terrorismos y por el uso frecuente (aunque no exclusivo) de perpetradores suicidas.” Véase: DE LA CORTE IBÁÑEZ, Luis (2012), opus cit., p. 35.

⁴⁹ “La fuerza y poder de los terroristas reside en que con sus actos parecen demostrar la incapacidad de los gobiernos para responder eficazmente, mostrando que se equivocan en el uso del poder existente” Véase: PALMERTON, Patricia Ruby «The rhetoric of terrorism and media responses to the ‘Crisis in Iran’», *Western Journal of Speech Communication*, 52:2, 105-121. Como se citó en: GARCÍA GURRIONERO, Mario (2013), opus cit., p. 38.

⁵⁰ El concepto terrorismo global “[...] puede aplicarse a cualquier terrorismo que, aprovechando las condiciones de interconexión económica, política, informativa y cultural que caracterizan al mundo globalizado del siglo XXI, cuente con la determinación y la capacidad necesarias para producir repercusiones (psicológicas, sociales, informativas y políticas) de alcance mundial.” DE LA CORTE IBÁÑEZ, Luis (2013): «¿Hasta qué punto convergen el terrorismo global y la criminalidad organizada? Parámetros generales y escenarios críticos», *Revista del Instituto Español de Estudios Estratégicos*, (1), p. 154.

⁵¹ “También podría denominarse ‘convergencia por apropiación de métodos’, y se trata de su forma más básica. Tiene lugar cuando grupos u organizaciones terroristas se involucran en actividades típicas de la criminalidad organizada. Nos referimos esencialmente a acciones delictivas de diferente índole, elegidas para satisfacer necesidades logísticas o de financiación.” *Ibidem*; p. 155.

El objetivo primordial del terrorismo es la alteración de la paz pública. Para ello se vale de la violencia y la espectacularidad de los atentados que comete a fin de lograr la implementación del terror en el seno de la sociedad.⁵²

10. Propaganda e ideología:

El terrorismo implica necesariamente el uso de la propaganda para la penetración de su mensaje en el tejido de la sociedad. Busca la legitimación de su ideología y la legitimación del uso de la violencia como único medio para la obtención de sus fines. Para ello utiliza diversos instrumentos propagandísticos con la finalidad de atraer la atención hacia su discurso.⁵³ Refiriéndose al yihadismo, De la Corte menciona que la propaganda actúa como el paso previo a la obtención de recursos económicos y materiales en cuanto ayuda a difundir la ideología del islamismo salafista radical y a captar grupos o personas que contribuyan con la yihad global.⁵⁴

Finalmente, es necesario consensuar dos aspectos relevantes relativos a este tema antes de continuar en nuestro estudio.

Primero, es posible referirse a terrorismo internacional siempre que se observe la prevalencia de las características descritos. Con base en la inexistencia de una definición común es relevante la caracterización de este fenómeno con el fin de evitar señalar como terrorismo, aquello que no lo es.

Segundo, muchos de los elementos previamente descriptos que determinan propiamente la génesis del terrorismo, encuentran en Internet un espacio idóneo para su máximo desarrollo. Por lo tanto, el uso de Internet por parte de los grupos terroristas, con especial incidencia en el terrorismo internacional, es un instrumento nuevo que facilita la expansión y multiplicación de sus fines en una modalidad sin precedentes.

⁵² “[...] el terrorismo suele involucrar una sucesión de actos violentos ejercidos con premeditación, principalmente sobre población no combatiente, orientados en primera instancia a generar un profundo impacto psicológico (intimidación, sorpresa, miedo, terror).” DE LA CORTE IBÁÑEZ, Luis (2012), opus cit., p. 34.

⁵³ “[...] los terroristas presentan un motivo sustancial para disenter de la política de un gobierno. Como saben que los motivos ambiguos y mal definidos probablemente no consigan atraer el mismo apoyo que los que están claramente planteados y conectados (es decir, contextualizados ideológica o históricamente, por ejemplo), los terroristas componen sus mensajes con fuerza suficiente para atraer la atención.” [...] “Los terroristas construyen con sus acciones discursos potentes, con mensajes claros y con una gran capacidad para atraer el foco de atención de la audiencia” [...] “En el marco del terrorismo actual los terroristas se esfuerzan por encontrar los motivos que les permitan justificar sus acciones criminales” [...] La ideología “da coherencia a la declaración y el pensamiento de los terroristas. En la base de todo grupo terrorista subyace la búsqueda por reinterpretar la sociedad y su sustancia”. GARCÍA GURRIONERO, Mario (2013), opus cit., p. 37-40.

“La propaganda terrorista reitera insistentemente la responsabilidad última de unos gobernantes, cuyas políticas abiertamente opresoras e inhumanas, han empujado hacia la violencia a unos individuos que no han podido resistir durante más tiempo el cúmulo de injusticias y ataques sufridos. El objetivo último es, pues, deslegitimar al enemigo, cuestionar las [...] razones que amparan al gobierno en su lucha contra el grupo y presentar como desproporcionadas y tiránicas las medidas políticas y policiales [...]”. TORRES SORIANO, Manuel R. (2007): *La dimensión propagandística del terrorismo yihadista global*. Tesis doctoral. Granada: Universidad de Granada, p. 65.

⁵⁴ DE LA CORTE IBÁÑEZ, Luis (2012), opus cit., p. 35-38.

CAPÍTULO 2: INTERNET COMO EL ESPACIO IDÓNEO PARA UNA NUEVA OPORTUNIDAD CRIMINAL

Hace décadas, el surgimiento de Internet supuso en principio que su uso fuera limitado a los espacios institucionales públicos, a las fuerzas y los cuerpos de seguridad del Estado, al mundo académico, al mundo empresarial, y a una contable cantidad de usuarios particulares. Con el surgimiento de las Nuevas Tecnologías de la Información y Comunicación (TIC) como nicho de investigación y desarrollo, el fortalecimiento del sector privado por medio de subvenciones y préstamos, el sistema educativo orientado a las nuevas demandas del mercado laboral, el subsidio a países en vías de desarrollo en materia tecnológica, el surgimiento de nuevos prestadores de servicios de software y desarrolladores de hardware, y las industrias vinculadas a los servicios online (principalmente la industria audiovisual y musical) se ha instaurado el escenario ideal para la digitalización del mundo. Todo ello, en su conjunto, ha impulsado la democratización de Internet, y su alcance, entonces, se ha vuelto plenamente extensivo. A partir de este hecho, se ha desencadenado un uso de Internet, por todos ya conocido, que se ha orientado no solo a la adquisición de bienes y/o servicios, sino también a la comunicación entre personas más allá de sus fronteras regionales.

Cabe afirmar que nuestro presente se ha configurado a través de esta comunicación múltiple y digital entre personas, desarrollando así un mundo altamente intercomunicado, lo que McLuhan denominó *Aldea Global*⁵⁵. Este hecho trajo indudables beneficios, pero de forma paralela también permitió la aparición de nuevos y diferentes problemas, como el crimen en el ciberespacio. Los medios de comunicación actuales y las agencias de noticias del mundo han dirigido el foco de atención hacia este binomio entre crimen e Internet, y por ello en los últimos cinco años aproximadamente hemos visto toda serie de noticias en torno a este nuevo fenómeno.

En el caso puntual del terrorismo, los crímenes que más se han reseñado por parte de medios y de investigadores académicos, han sido los que realizan las organizaciones terroristas con fines propagandísticos. En el terrorismo yihadista, este uso es muy profuso y se encuentra ampliamente estructurado⁵⁶, pero no representa el único uso criminal de Internet por parte del yihadismo, y, definitivamente, la utilización de canales comunicativos con fines de difusión no representa un uso novedoso.

El terrorismo siempre ha buscado publicitar sus acciones. Para la difusión de sus atentados o de sus mensajes, el terrorismo de antaño se valía de la televisión de igual forma que hoy en día se vale de Internet. El terrorismo, por tanto, se beneficia de cualquier avance tecnológico que impacte en el desarrollo de canales comunicativos. Bowyer Bell ha destacado la vinculación

⁵⁵ El concepto de Aldea Global aparece por vez primera descrito por McLuhan en los textos denominados *The Gutenberg Galaxy* (1962) y *Understanding Media* (1964). Para McLuhan, la nueva interdependencia electrónica crea el mundo a imagen de una aldea global. Se refería por esto a la idea de que la tecnología estrechaba espacios y ponía de relevancia el carácter humano de las relaciones. Sin embargo, en una entrevista televisada en los años '60, McLuhan afirma que "*la aldea global es un mundo en el cual no necesariamente tienes armonía*." Véase: AYALA PÉREZ, Teresa (2012): «Marshall McLuhan, las redes sociales y la Aldea Global», *Revista Educación y Tecnología*, N.º 2, pp. 8-20.

⁵⁶ La propaganda yihadista en Internet posee una segmentación del mensaje acorde a diversos parámetros previamente definidos por los propios grupos yihadistas. Estos parámetros habitualmente son: tipos de públicos a los que va dirigido el mensaje, intención del mensaje, canal que se utiliza para divulgar el mensaje, etc.

entre el terrorismo y la modernización de los medios⁵⁷. Este autor sostiene que el impacto masivo de la acción terrorista se debe a la inmediata divulgación del horror. Esta búsqueda de publicidad llega a constituir la propia génesis del terrorismo, y llega a producir una “relación simbiótica”⁵⁸ entre el terrorismo y los medios de comunicación. Tal es la relación, que este autor se refiere en sus análisis a los grupos terroristas como a los “terroristas de la televisión”.⁵⁹

Los medios de comunicación tradicionales⁶⁰ siempre han tenido un lugar determinante en la difusión de las noticias relacionadas con el yihadismo en Internet. De este modo, con independencia del mundo académico y del universo penal que siempre han buscado analizar y reprimir este fenómeno respectivamente, en el presente, una gran mayoría de la población posee alguna idea de la relación que ya existe entre el terrorismo e Internet.

Según *The European Commission's Expert Group on Violent Radicalisation*, el terrorismo habitual, que siempre se ha caracterizado por la búsqueda de la espectacularidad y la publicidad de sus atentados en los medios de comunicación tradicionales, ha dado paso a una nueva forma de terrorismo, personificada en el yihadismo, que centra sus esfuerzos en la promoción de su ideología por medio de Internet. Esto posee inmediatas ventajas dado que las Nuevas Tecnologías de la Información y la Comunicación (TIC) permiten controlar la creación y distribución del mensaje, sin que el contenido de este sea sometido a censura por parte de los medios de comunicación tradicionales, lo que facilita la promoción del mensaje yihadista con fines de captación, incitación y radicalización hacia el terrorismo.⁶¹

Esta difusión continuada y sostenida de mensajes en la red con retórica violenta no solo busca incentivar los actos de violencia, sino que también busca desarrollar una narrativa extremista de hondo calado que fomente, de forma dirigida, una única interpretación del Islam. Por tanto, se debe partir de la base de que cuando se habla de *narrativa terrorista online* se debe necesariamente hacer referencia al discurso propagandístico del cual hacen uso algunos grupos yihadistas con fines de reclutamiento, incitación al terrorismo y radicalización, y que está estratégicamente construido con orientaciones específicas hacia los diversos públicos en los que se enfoca.

La particularidad que aporta Internet entonces como instrumento de uso por el terrorismo (y principalmente la utilización de las redes sociales y otros canales digitales como son los blogs, periódicos en línea, páginas webs y revistas online de actual pertenencia al yihadismo) es que permite controlar el mensaje desde su creación hasta la difusión del mismo, y no está sujeto, en consecuencia, a una censura y/o interpretación externa, como sí sucede con los medios tradicionales.

⁵⁷ Nótese que por *modernización* el autor se refiere a los saltos cualitativos que se produjeron durante el desarrollo de la televisión, y que resultan contextuales a la época de sus estudios.

⁵⁸ BOWYER BELL, John (1978): *A time of terror*. New York: Basic Books, p. 110.

⁵⁹ *Ibidem*; p. 4.

⁶⁰ Léase: Radio, prensa y televisión.

⁶¹ EUROPEAN COMMISSION'S EXPERT GROUP ON VIOLENT RADICALISATION (2008): *Radicalisation processes leading to acts of terrorism* (Report), Brussels: European Commission, pp.1-21.

Según Noam Chomsky y Edward Herman, “los medios de comunicación [tradicionales] actúan como un sistema de transmisión de mensajes y símbolos para el ciudadano común”.⁶² Este sistema de transmisión de mensajes escoge a priori qué información brindar al ciudadano, cuándo y cómo hacerlo. Ello significa que puede modificar, interpretar y/o censurar algún contenido específico de un hecho noticioso. O censurar, incluso, la totalidad del hecho noticioso y así impedir el acceso a una información concreta al público. El tratamiento informativo de las noticias sobre terrorismo están también sujetas a esta racionalización de los medios de información. Cuando los terroristas manifiestan la intención de enviar un mensaje a la población, a un gobierno, a un mandatario específico, (mediante un atentado, un video, un manifiesto, etc.) esta intención puede verse alterada por este sistema de transmisión de mensajes al que hace referencia Chomsky y Herman. Se entiende de ello que, entre la creación de un mensaje (por ejemplo, un video de 35 minutos de reivindicación sobre un atentado en una ciudad) por parte de un grupo yihadista y su visionado por una audiencia televisiva, existe un proceso intermedio que puede distorsionar el significado del mismo. Este proceso intermedio es llevado a cabo por parte del medio de comunicación que actúa como un enlace, o como un interlocutor, entre el grupo terrorista y el público. Ello puede modificar (intencionadamente o no) el mensaje original. Si tenemos en cuenta entonces que en la emisión de información puede tener lugar una interpretación (que actuará a su vez a modo de traducción hacia el espectador), o una censura en la emisión de alguna parte del video, la intencionalidad de este video se verá alterada.

Por el contrario, el uso de Internet no solo facilita el enlace directo entre el productor y el consumidor del mensaje, sino que también asegura el control sobre su significado dado que el contenido del mensaje escapará al control impuesto por los medios de comunicación. De esta forma el emisor primigenio (en este caso el grupo terrorista) poseerá la certeza de que el contenido discursivo del mensaje no estará sujeto a interpretaciones o ediciones de terceros. Este control absoluto del mensaje ha llevado a los grupos yihadistas a desarrollar sus propias páginas webs, blogs, revistas online, muros en redes sociales, y otros formatos digitales con el fin de difundir su propaganda. Cada uno de esos sitios actúa en el ciberespacio como una herramienta comunicativa propia que facilita la difusión de la ideología.⁶³ Tal como indicó Marín Dueñas, P.P., y Lasso de la Vega González, M.C.,

«El site organizacional pasa a ser una herramienta imprescindible para todas las personas que se relacionan con ella configurándose, a su vez, como un instrumento básico para las organizaciones, proporcionando, entre otras, las siguientes oportunidades y beneficios, [...] influye en la imagen y credibilidad; permite la comunicación bidireccional, posibilidad de hablar directamente con los públicos; facilita el acceso al público objetivo, [...] elimina los intermediarios; elimina las restricciones geográficas: las organizaciones están a un solo *click*, permiten dar a conocer a la organización a públicos que pueden estar en sitios muy lejanos; hace más eficaz la comunicación, permitiendo desarrollar y construir relaciones más directas, personalizadas y a largo plazo; permite dirigirse a cada consumidor con un mensaje personalizado» [...].⁶⁴

⁶² CHOMSKY, Noam/HERMAN, Edward, S. (2000): *Los guardianes de la libertad: propaganda, desinformación y consenso en los medios de comunicación de masas*. Barcelona: Crítica, p. 21.

⁶³ En el Capítulo 3 de esta tesis se abordará en profundidad esta temática. En dicho capítulo se llevará a cabo un análisis comunicativo sobre la yihad que desarrolla en Internet el autoproclamado Estado Islámico.

⁶⁴ MARÍN DUEÑAS, Pedro Pablo/LASSO DE LA VEGA GONZÁLEZ, María del Carmen (2017): «La efectividad de las páginas web en la comunicación empresarial de las pequeñas y medianas empresas. Un estudio en PYMES de la provincia de Cádiz», *ZER: Revista de Estudios de Comunicación = Komunikazio Ikasketen Aldizkaria*, 22(42).

Este es, entre otros, uno de los motivos por los que el terrorismo yihadista utiliza Internet de forma propagandística.

Para el terrorismo yihadista, el uso de Internet con fines propagandísticos posee dos vertientes. Por un lado, se encuentra la propaganda que se dirige a la población occidental cuyo contenido está orientado a generar preocupación y temor en la población de determinados Estados; y por el otro, la propaganda dirigida a los simpatizantes o población afín, cuyo contenido está orientado al reclutamiento y/o radicalización con independencia de la región geográfica del destinatario de estos mensajes.

En el primer caso, el uso de la violencia o la amenaza del uso de la violencia por parte de un grupo yihadista que utiliza Internet genera el mensaje indiscriminado de terror y la ampliación de sus manifestaciones violentas. Como mencionábamos antes, las Nuevas Tecnologías de la Información y Comunicación (TIC) permiten controlar la creación y distribución del mensaje, sin que el contenido de este sea sometido a censura por parte de los medios de comunicación tradicionales. Bajo esta modalidad, se promueve la publicación y distribución de mensajes en la red de forma indiscriminada cuyo único objetivo es denotar presencia, sin establecer una distinción en el receptor o receptores de dichos mensajes.

En el segundo caso, el mensaje está orientado a la propaganda con fines de reclutamiento y/o radicalización, y este mensaje propagandístico a su vez se encuentra segmentado en diversas variables que tienden a la atención de diversos públicos, con diversas motivaciones, y que son ideologizados por medio de diversos formatos electrónicos. De esta forma, mediante la legitimación de las acciones de violencia, mediante el establecimiento de una única interpretación del islam y mediante el autoadoctrinamiento se produce un incremento de los atentados terroristas llevados a cabo por los denominados “lobos solitarios”, es decir, sujetos en los que la combinación Internet + propaganda yihadista surte especial efecto de cometidos violentos.

¿Qué aporta Internet en todo este proceso propagandístico? La propaganda yihadista en Internet posee una importancia determinante en la configuración del nuevo terrorismo. Internet aporta al proceso propagandístico elementos que son propios de la naturaleza de este medio, como el anonimato, la ampliación de la red de distribución del mensaje, la rapidez en la diseminación del mismo y la existencia de *echo chambers*.

El primer aporte que realiza Internet al proceso propagandístico es el anonimato, debido al hecho de que el sujeto delictivo se encuentra *a priori* a cubierto tras un ordenador y/o protegido mediante números de IP enmascarados. Debe tenerse en cuenta el hecho de que actualmente constituye delito la propaganda tendiente a la captación, adiestramiento o adoctrinamiento online⁶⁵. En el caso de España, el 30 de marzo de 2015 tuvo lugar la aprobación y sanción de la Ley Orgánica 2/2015, en materia de delitos de terrorismo.⁶⁶ La LO 2/2015 incorpora, en torno

⁶⁵ MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA (2015): *Plan Estratégico Nacional de Lucha contra la Radicalización Violenta* (PEN-LCRV), de 30 de enero.

⁶⁶ Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

a la tipificación, nuevos delitos de terrorismo⁶⁷ (consistentes en la captación, adiestramiento o adoctrinamiento por medio de Internet), y adicionalmente, modificaciones en el enfoque político-institucional al establecer por medio de esta normativa al terrorismo como un asunto de Estado,⁶⁸ lo que a su vez ha permitido el aumento de las penas privativas de libertad. Por lo tanto, el anonimato que aporta Internet para la comisión de este tipo de delitos resulta de sumo beneficio para esta modalidad criminal.

El segundo aporte que realiza Internet al proceso propagandístico es la ampliación de la red de distribución del mensaje. Mediante el uso de las nuevas tecnologías el individuo, que es potencial sujeto de reclutamiento o radicalización, está expuesto no solo al mensaje propagandístico de la fuente primaria, sino también a las réplicas del mensaje realizadas por otros receptores de este. Ello amplía la red de distribución del mensaje y por tanto maximiza su efecto en la diseminación de este. Debe también considerarse el hecho de que esta ampliación de la distribución está dada en gran medida por la diversidad de formatos electrónicos existentes para la distribución de un mismo mensaje.

El tercer aporte está dado por la rapidez. Según Miguel Ángel Cano Paños,⁶⁹ la rapidez es uno de los elementos determinantes que establece una diferencia respecto a la distribución de la propaganda antes y después de la existencia de Internet, es la inmediatez del mensaje. Esta inmediatez incide de manera significativa no solo en la rapidez de distribución del mismo, sino que también actúa acortando los periodos de adoctrinamiento.

Finalmente, el cuarto aporte que realiza Internet a este proceso propagandístico es la existencia de las denominadas *echo chambers*. Internet genera el encuentro de personas con las mismas ideas o intereses. Si bien en el ámbito de las telecomunicaciones el término posee diversos significados, el más habitual se refiere al desarrollo de software que mediante algoritmos recoge la navegación de un usuario de Internet para ofrecerle contenido de similares características. De esta manera, el software procesa los intereses o búsquedas del navegador para ofrecer permanentemente contenido idéntico al buscado en un inicio. De esta forma se generan las denominadas *echo chambers*, que en el caso del terrorismo yihadista tienden al aumento del extremismo, dado que las *echo chambers* son espacios o situaciones de reforzamiento de ideas mediante la repetición de intereses similares, reforzando de esta manera y en este caso puntual, el sistema de creencias del individuo radicalizado o por radicalizar.

Cabe señalar que el uso de Internet no solo es relevante por las facilidades que otorga al yihadismo sobre el control del mensaje para el desarrollo de su estrategia comunicativa. Debe tenerse en cuenta también que Internet es, debido a su naturaleza anónima, un escenario que se adecua a los múltiples fines criminales de los grupos terroristas. Es por ello por lo que actualmente la relación que puede establecerse entre el terrorismo e Internet es muy variada, y

⁶⁷ Delito de adoctrinamiento y adiestramiento militar (art. 575), delito de adoctrinamiento pasivo (art. 575.2), delito de enaltecimiento o justificación pública de los delitos de terrorismo (art. 578), y delito de incitación al terrorismo (art. 579).

⁶⁸ DIARIO LA LEY (2015). Comentario a la LO 2/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. (BOE 31 de marzo de 2015), Sección documento online, N.º 8511, Editorial La Ley; p. 1.

⁶⁹ CANO PAÑOS, Miguel Ángel (2008a): «Internet y terrorismo islamista. Aspectos criminológicos y legales», *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, diciembre (22), pp. 67-88.

está compuesta casi exclusivamente por hechos delictivos.⁷⁰ Estas acciones delictivas han sido explicadas por variedad de disciplinas científicas.

Puntualmente, en la ciencia criminológica actualmente existen numerosas teorías que explican, o tratan de explicar, el crimen y los fenómenos adyacentes al mismo. Ello ha ido conformado en esta disciplina un gran constructo teórico que se ha ido materializando lentamente y que ha tenido su impulso más importante en los últimos treinta años. Dentro de esta profusión de teorías que han tenido lugar en esta área científica, se debe rescatar especialmente a las teorías de la oportunidad, debido a que estas se han dedicado a estudiar a las condiciones ambientales que favorecen el delito como una de las variables determinantes para la comisión de este.

De acuerdo con las teorías de la oportunidad, sobre las cuales ahondan ampliamente Felson y Clarke, el comportamiento individual es producto de una interacción entre la persona y su entorno físico. Esto quiere decir que ciertos escenarios pueden ayudar a convertir las inclinaciones delictivas de ciertos individuos en acción. En otras palabras, ciertos entornos favorecen el delito. De esta forma se entiende que Internet es un espacio idóneo para una nueva oportunidad criminal porque contiene en el anonimato la condición necesaria para que el delito suceda. Según Felson y Clarke⁷¹, la navegación anónima en la red ayuda a hacer aún más consistente esta oportunidad de dos formas: por un lado, incita a más personas a cometer delitos⁷² y, por el otro, ayuda al delincuente a ser más eficiente en su labor.⁷³ Podremos ver más claramente este último aspecto si tenemos en cuenta los seis principales usos de Internet que realizan los grupos terroristas según lo descrito por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que se desarrollarán en el capítulo siguiente.

Para Felson y Clarke, las teorías de la oportunidad del delito son aquellas que se sustentan en el siguiente principio: “las oportunidades fáciles o tentadoras atraen a la gente a la acción delictiva”.⁷⁴ Entre las teorías de la oportunidad delictiva en las que profundizan estos autores encontramos la teoría de las actividades cotidianas (TAC), la teoría del patrón delictivo y la teoría de la elección racional.

La *teoría de las actividades cotidianas (TAC)* parte de la idea de que los crímenes tienen lugar cuando convergen tres elementos básicos: un delincuente motivado, un objetivo apropiado y la ausencia de un vigilante eficaz. En este enfoque se desplaza el centro de atención desde el delincuente hacia el objetivo o hacia el vigilante. Entiende por tanto que no es tan importante el delincuente y sus causas, sino la vigilancia frecuente que asume como altamente disuasoria. Así,

⁷⁰ “Internet [...] se ha convertido en un instrumento de difusión de propaganda.” Véase: JORDÁN, Javier/TORRES SORIANO, Manuel R. (2007): «Internet y actividades terroristas: el caso del 11-M», *Revista Profesional de la información*, (2)16, marzo de 2007, p. 129.

⁷¹ FELSON, Marcus/CLARKE, Ronald (1998): «Opportunity makes the thief. Practical theory for crime prevention», *Research, Development and Statistics*, Police Research Series Paper N° 98, London.

⁷² Un ejemplo de esto se ilustra con un ciudadano cualquiera que comienza de forma espontánea a radicalizarse por medio del consumo continuado de publicaciones yihadistas en Internet. Este acto, en apariencia inofensivo, determina en sí mismo un delito en el ámbito de la Unión Europea, y se encuentra actualmente tipificado en España como delito de adoctrinamiento pasivo (art. 575.2 CP).

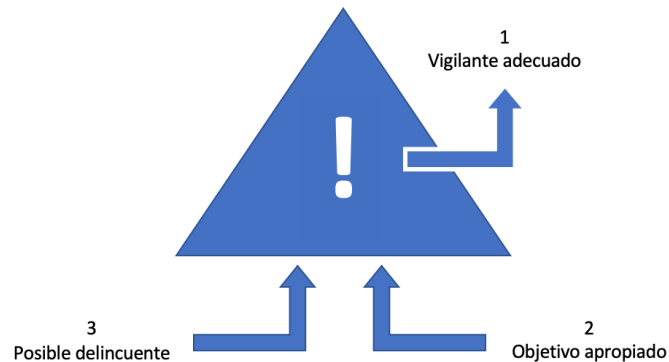
⁷³ En el caso de la criminalidad transnacional, y en nuestro caso puntual sobre terrorismo yihadista cabe destacar que Internet favorece y simplifica, desde un punto de vista técnico, la eficacia de las acciones delictivas.

⁷⁴ *Ibidem*, p. 2.

la presencia o proximidad, de un vigilante adecuado⁷⁵ disuade al delincuente de llevar a cabo su cometido.

Tomando como base el triángulo del delito, Felson ha dejado esquematizado este enfoque en el siguiente gráfico:

Gráfico 1: Teoría de las actividades cotidianas y el triángulo del delito.



Fuente: Felson, Marcus. 1998. *Crime and Everyday Life*. Second edition. Thousand Oaks, CA: Pine Forge Press.

En este esquema, Felson sintetiza la teoría en la idea central de que un delito tiene lugar cuando coinciden en un mismo espacio y tiempo⁷⁶, un posible delincuente y un objetivo apropiado. Y es, puntualmente, un guardián eficaz quien con su presencia disuade el delito, o con su ausencia facilita la comisión de este.

Cabe señalar que este enfoque, si bien se estableció inicialmente como una explicación para aquellos delitos depredatorios⁷⁷, en la actualidad puede ser aplicado a una variedad de delitos y de entornos cada vez más complejos, como es el caso de Internet.

Miró Llinares ha desarrollado ampliamente este supuesto al realizar un análisis de la cibercriminalidad partiendo de la hipótesis de que este nuevo ámbito conlleva cambios esenciales en todos los eventos, y entre ellos, sobre el crimen.⁷⁸ Este autor plantea que, si bien han aparecido nuevos delitos, que son propios al surgimiento y a la naturaleza de Internet, existen otros delitos que ya se conocían y cuya comisión solo cambia de lugar.

Partiendo de esta premisa, podemos hablar entonces de la Tecnología Informática (TI) como objeto o como medio. Es decir, entender a la informática como un *objeto del delito*, o como un *medio para el delito*. La primera modalidad es aquella que solo tiene lugar en el ciberespacio.

⁷⁵ Este enfoque teórico entiende por *vigilante adecuado* o *guardián eficaz* no necesariamente un policía o guarda de seguridad, sino a alguien (o algo) que desmotive la comisión del delito con su sola presencia: un ama de casa, vecino, portero, compañero de trabajo, un desconocido en un sitio público, buena iluminación en los alrededores, alarma, etc., es decir, cualquier individuo o sistema que permita que el objetivo no quede expuesto. Con esta figura básicamente, Felson y Clarke se refieren a la ausencia o la existencia de control.

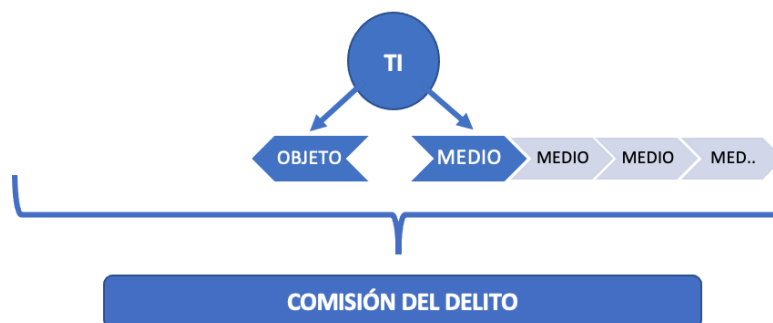
⁷⁶ Este espacio físico-temporal de confluencia se representa simbólicamente con un triángulo. Es lo que se conoce como Triángulo del Delito.

⁷⁷ Robo con violencia y daño; saqueo; devastación; malversación de caudales; exacción ilegal con abuso de poder y confianza.

⁷⁸ MIRÓ LLINARES, Fernando (2011): «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», *Revista Electrónica de Ciencia Penal y Criminología (RECPC)*, pp.1-55.

Entrarían en esta categoría todos los delitos nacidos a partir del surgimiento de Internet, y sin cuya tecnología sencillamente no existirían.⁷⁹ La segunda modalidad engloba delitos que pueden ser cometidos tanto en el espacio físico como en el espacio digital. Entrarían en esta categoría aquellos delitos que ya se hayan recogidos en diversas legislaciones nacionales como tipos penales existentes y, en cuyo caso, deben adoptar particularidades criminológicas y/o penales diferentes, y propias del nuevo entorno.⁸⁰

Gráfico 2: La tecnología informática como objeto y como (nuevo) medio del delito.



Fuente: Elaboración propia. 2022.

Dentro de esta segunda categoría, en la que se utiliza la TI como medio, se pueden encontrar una serie de delitos caracterizados por la divulgación de contenido ilícito. Tal es el caso de la difusión en línea de textos, imágenes o videos online continentales de abuso sexual infantil⁸¹, a

⁷⁹ Son los llamados delitos tecnológicos o *high-tech crimes*., cuyo objetivo son los sistemas informáticos o tecnologías de la información, como, por ejemplo, hackeo, crackeo, ataques DoS, envío de malware o ataques *ransomware* (WannaCry), etc.

⁸⁰ Por ejemplo, ciberestafas, *cyberbullying*, *grooming*, *sexting*, *carding*, *phishing*, *vishing*, etc. Son delitos que se llevan a cabo mediante computadoras o redes como Internet. Estos delitos son denominados *e-Crimes*.

⁸¹ Interpol indica que es preciso referirse a abuso sexual infantil, y no a pornografía infantil, a fin de seguir las “orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexual, también conocidas como las Orientaciones de Luxemburgo. Estas ofrecen una directriz clara sobre cómo guiar el complejo léxico normalmente utilizado al hablar de explotación y abusos sexuales de menores. Las Orientaciones de Luxemburgo fueron elaboradas por un grupo de 18 socios internacionales” [quienes consideran que] “términos [como pornografía infantil] no deberían formar parte del lenguaje legítimo utilizado por los organismos encargados de la aplicación de la ley, la judicatura, el público o los medios”, debido a que ‘pornografía’ es un término que implica la práctica sexual consensuada, y la distribución de dichos actos de forma habitualmente legal. Véase: INTERPOL. *Alentamos el uso de terminología apropiada para evitar banalizar el abuso y la explotación sexual de niños*. Disponible en: <https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada> [Fecha de consulta: 23 de noviembre de 2023].

Según María Inmaculada Ramos Tapia, este término también es recogido en diversos instrumentos normativos, entre ellos, el «Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (ratificado por España el 22 de julio de 2010, publicado en BOE de 12 de noviembre de 2010) que obliga a tipificar [en su art. 18] “[...] como abuso sexual la conducta del que realiza actos sexuales con un niño “abusando de una posición reconocida de confianza, autoridad o influencia sobre el niño, incluso en el seno de la familia; o abusando de una situación de especial vulnerabilidad del niño, en particular debido a una discapacidad psíquica o mental o una situación de dependencia”. Véase: RAMOS TAPIA, María Inmaculada (2013): «Delitos de abusos sexuales a menores: arts. 182, 183 y 183 bis», en: ÁLVAREZ GARCÍA, Francisco Javier (Dir.) /DOPICO GÓMEZ-ALLER, Jacobo (Ed.), *Estudio crítico sobre el Anteproyecto de reforma penal de 2012*, Valencia: Tirant lo Blanch, p. 660.

Cabe señalar que la consideración de ‘menor de edad’ está dada en España por la Ley Orgánica 1/2015, de 30 de marzo, por la cual se establece un aumento en la franja de edad para consentir libremente la realización de actividades sexuales, situándose la misma en 16 años (previo a esta reforma de 2015, que modifica el Código Penal de 1995, se situaba en 13 años) y estableciendo de esta forma una mayor protección a los menores. Véase: RAMOS TAPIA, María Inmaculada (2015): «La tipificación de los abusos sexuales a menores: el proyecto de reforma de 2013 y su adecuación a la Directiva 2011/92/UE», en: VILLACAMPA ESTIARTE, Carolina/AGUADO-CORREA, Teresa (Coords.), *Delitos contra la libertad e indemnidad sexual de los menores*, Aranzadi, Pamplona, pp. 107-137.

los discursos de odio en la red⁸² y, por supuesto, el uso de Internet por parte del terrorismo yihadista.

Esta promoción de delitos en Internet se facilita, según la teoría de las actividades cotidianas (TAC) a la que nos venimos refiriendo, por la ausencia de lo que Felson denomina ‘vigilantes o guardianes eficaces’. Debe de tenerse en cuenta que, si bien una parte de esta actividad es reprimida por las Fuerzas y Cuerpos de Seguridad de un Estado, por diversas organizaciones y agencias de vigilancia nacional, regional e internacional⁸³, empresas públicas y privadas⁸⁴, y por un gran número de ciudadanos organizados para la vigilancia de Internet⁸⁵, existe un altísimo porcentaje de publicaciones digitales que tienen lugar en la *Dark Web*⁸⁶, y que por lo tanto resultan indetectables a este ‘vigilante eficaz’ en una navegación habitual. Este hecho

Con independencia de la recomendación internacional sobre la utilización del término ‘abuso’, cabe señalar que en el año 2022 ha tenido lugar la adopción en España de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual. Esta ley, denominada por el Ministerio de Igualdad como ley del “solo sí es sí”, entre otros cambios normativos, elimina “*el abuso sexual como tipo penal específico. Esto no quiere decir que se despenalice, sino que se equipara abuso sexual con agresión sexual.*” Véase: «Cambios en el Código Penal tras la aprobación de la ley del “solo sí es sí”», Gerson Vidal Rodríguez, 29 de mayo de 2023. Disponible en: <https://www.gersonvidal.com/blog/cambios-codigo-penal-ley-solo-si-es-si/> [Fecha de consulta: 13 de diciembre de 2023].

⁸² Los discursos de odio o *hate speeches* se encuentran regulados en el art. 510 del Código Penal [español], bajo la tipificación de delito de odio. El delito de odio consiste en un acto penal contra una o varias personas por el hecho de pertenecer a un determinado grupo social. El delito es aplicable a aquellos que “*públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad*” (art. 510.1.a); o que “*produzcan, elaboren, posean con la finalidad de distribuir, faciliten a terceras personas el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos*” (art. 510.1.b) para la comisión de este delito. También a quienes “*públicamente nieguen, trivialicen gravemente o enaltezcan los delitos de genocidio, de lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado*” (art. 510.1.c); a quienes “*lesionen la dignidad de las personas mediante acciones que entrañen humillación, menosprecio o descrédito*” (art. 510.2.a) contra uno de los grupos protegidos o contra una de las personas por razón de su pertenencia a estos grupos; y a quienes “*enaltezcan o justifiquen por cualquier medio de expresión pública o de difusión los delitos que hubieran sido cometidos contra un grupo*” (art. 510.2.b). Finalmente, el art. 510.3 determina que “*las penas previstas en los apartados anteriores se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas.*”

⁸³ Internet Crime Complaint Center (IC3), International Criminal Police Organization (Interpol), European Union Agency for Law Enforcement Cooperation (Europol), Joint Cybercrime Action Taskforce (J-CAT), National Security Agency (NSA) -por medio de ECHELON, XKeyscore, PRISM y UPSTREAM-, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), European Cybercrime Centre (EC3), Government Communications Headquarters (GCHQ) – por medio de Tempora -, Five Eyes (FVEY), United States Department of Defense, Defense Intelligence Agency (DIA) – por medio de HUMINT y MASINT, National Reconnaissance Office (NRO) - por medio de SIGINT y MASINT-, etc.

⁸⁴ INSO Group (Israel) – por medio de Pegasus -, Internet Eyes (Reino Unido), Huawei y ZTE (China) – ambas empresas por medio de DPI: Deep Packet Inspection -, Blue Coat Systems (USA), Gamma International (Reino Unido y Alemania) – por medio de FinFisher, y Trovicor (Alemania), etc.

⁸⁵ Programa Cibercooperantes del Instituto Nacional de Ciberseguridad (España), Texas Virtual Border Watch (USA), National Security Alliance (USA), etc.

⁸⁶ Internet suele representarse habitualmente con el gráfico de un iceberg. Teniendo en cuenta esta ilustración, lo primero que hay que señalar es que la gran mayoría de los usuarios de Internet navegan en la superficie de este iceberg, cuya zona se denomina *Clearnet*. Se trata de una parte visible de la red a la cual se accede a páginas e información ubicadas fácilmente mediante buscadores como Google, Yahoo, etc. Esta capa visible es la que explora el 90% de la población mundial y solo ocupa entre un 4% y un 10% del contenido total existente en la red. De este modo, la *Deep Web* es toda la masa de información que no está visible y que no es de acceso público. En la *Deep Web* se encuentran, por ejemplo, las bases de datos confidenciales de empresas e instituciones, carpetas de archivos de Dropbox o Google Drive, foros privados, etc. Cabe señalar que la *Deep Web* no implica necesariamente la existencia de una actividad delictiva, se trata más bien de información sensible o de carácter privado. La actividad delictiva propiamente dicha (compraventa de armas, de drogas, de órganos humanos, de explosivos, pederastia, terrorismo, sicarios, y un sinnúmero de acciones criminales) la encontramos en la *Dark Web*, dado que es en esta última capa de Internet donde la información se oculta intencionalmente a fin de desarrollar todo tipo de ilícito. La *Dark Web* (o *Dark Net*) es una parte específica de la *Deep Web* que representa solo el 0,1% del total del iceberg de Internet. Este segmento reducido de información posee dominios propios y su navegación solo es posible por medio de programas específicos como Tor (u otros) que facilitan una navegación anónima. Es precisamente este anonimato del usuario y del productor de contenido online lo que multiplica exponencialmente las actividades delictivas en este micro segmento.

incrementa la comisión de los delitos previamente clasificados debido a que representa, en principio, una oportunidad fácil o tentadora de una acción delictiva.

Cabe señalar que la TAC es una teoría que centra uno de sus puntos de análisis en la evolución de la tecnología como variable medible de la modernidad en las sociedades.⁸⁷ Y que es precisamente esta modernidad y su evolución tecnológica lo que lleva a que exista una disminución progresiva de los vigilantes eficaces, con el consecuente aumento de las tasas de criminalidad.

Dentro de las teorías de la oportunidad delictiva, es necesario también reseñar en este análisis a la *teoría del patrón delictivo*. La teoría del patrón delictivo afirma que la distribución de los delitos no se produce al azar ni de manera uniforme, sino que existe un patrón. Por medio de esta teoría se explica cómo adquiere especial relevancia el lugar de confluencia entre el delincuente y la víctima. Estas ubicaciones, lugares o espacios, en donde se cruza la actividad cotidiana de una posible víctima y la actividad de un delincuente, se denominan nodos. Se caracterizan por ser áreas de alta oportunidad para cometer un acto delictivo y sobre las cuales los delincuentes poseen plena conciencia de su existencia, aunque no necesariamente las potenciales víctimas. Esta conciencia, sobre la existencia de lugares en donde resulta más fácil cometer un delito, lleva a los delincuentes a desarrollar patrones de comportamiento. Y es, debido precisamente a estos patrones de comportamiento delictivos, por lo que esta teoría resulta una herramienta de amplia predicción científica del crimen.

¿Cómo se aplica esto a nuestro estudio sobre Internet? Teniendo en cuenta a la red como un nodo, es decir, como un nuevo espacio para la oportunidad criminal recurrente. Naturalmente, esta afirmación no resulta en nada novedosa. Desde hace ya varias décadas se desarrollan programas de vigilancia en Internet a fin de frustrar nuevas oportunidades delictivas. No obstante, pese a los esfuerzos de organismos de vigilancia y control, de las regulaciones normativas estatales, y de campañas de prevención orientadas a la ciudadanía, el crimen en la red aumenta cada año de forma exponencial. Las estadísticas de Europa y Estados Unidos de América sobre delitos cometidos mediante el uso de la red denotan, en la última década, una marcada tendencia alcista.⁸⁸ Es esta tendencia alcista, precisamente lo que nos permite identificar a Internet como un nodo porque este crecimiento continuo da cuenta de patrones de comportamiento delictivo.

Internet resulta un espacio idóneo para la comisión delictiva, por su rapidez tecnológica, el anonimato propio su usabilidad y la amplitud de su alcance. La rapidez hace que el cibercrimen crezca a un ritmo acelerado. Según el reporte anual de Internet Crime Complaint Center (IC3)⁸⁹, los crímenes en Internet registrados han pasado de 16.838 (año 2000), a 303.809 (año 2010), a 4.2 billones (año 2020). En Latinoamérica, el Reporte de Ciberseguridad 2020⁹⁰ da cuenta de

⁸⁷ FELSON, Marcus/BOBA, Rachel (2009): *Crime and everyday life*. Newcastle: Sage Group.

⁸⁸ Esta afirmación deriva de la información analizada en los reportes anuales de *Internet Crime Complaint Center* (Estados Unidos) entre los años 2000 y 2020; y de la historiografía de datos del crimen en la red del Informe IOCTA 2021 (Unión Europea).

⁸⁹ IC3 es una iniciativa conjunta entre el FBI, el Centro Nacional para la Criminalidad de Cuello Blanco (NW3C), y la Oficina de Asistencia a la Justicia (BJA), USA. Desarrolla sus operaciones desde el año 2000.

⁹⁰ BANCO INTERAMERICANO DE DESARROLLO (BID)/ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA) (2020): *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Disponible en:

un incremento, respecto de la primera edición del año 2016, del número de usuarios de Internet en la región, y a su vez identifica que este hecho ha facilitado las vulnerabilidades en el campo digital. En este sentido, el ESET Security Report (ESR)⁹¹ recoge en un último informe el panorama de la seguridad corporativa en esta región y destaca que los ataques a los servicios de acceso remoto como RDP crecieron un 704%. Por su parte, el Informe IOCTA 2021 sobre la delincuencia organizada en Internet⁹², un valioso reporte anual de Europol que identifica la evolución del cibercrimen en la Unión Europea, describe cómo esta agencia ha registrado un aumento de sus operaciones transfronterizas de alto perfil contra amenazas cibernéticas, pasando de 57 operaciones en el 2013 a 430 operaciones en 2020. E identifica especialmente a los dos últimos años como un segmento temporal en el que se han disparado las amenazas producto del teletrabajo prolongado a causa de la pandemia de COVID-19. Finalmente, en España, informes propios identifican que tuvo lugar un incremento porcentual equivalente. De acuerdo con el Estudio sobre la Cibercriminalidad en España, en el año 2016 se registraron 92.716 delitos informáticos. En el 2019 esta cifra fue de 218.302 y en el año 2020 de 287.963.⁹³

Estos datos dan cuenta de que el constante desarrollo de las nuevas tecnologías permite a los delincuentes perfeccionar su accionar y agilizar la comisión de los delitos. En adición, este desarrollo constante de las TIC permite coordinar ataques cada vez más complejos o realizar otros usos criminales de la red en cuestión de minutos. Esta situación obliga a las Fuerzas y Cuerpos de Seguridad del Estado, a las Organizaciones Intergubernamentales y a las Agencias de Inteligencia a estar permanentemente actualizados con el fin de compensar esta velocidad de la comisión delictiva digital.

Finalmente, por medio de la *teoría de la elección racional* se explica una forma diferente de oportunidad delictiva que no atiende a los elementos circunstanciales de un potencial delincuente, sino al sujeto mismo. El actor individual es aquí la unidad de análisis. Y este análisis parte de la idea de que los individuos son egoístas y que actúan racionalmente para maximizar su bienestar.⁹⁴

La *teoría de la elección racional* estipula que el comportamiento delictivo de un individuo se explica por medio de una decisión racional. El crimen es consecuencia de una elección consciente, lo que se traduce en el hecho de que las personas adoptan decisiones sobre si perpetrar, o no, un delito. El comportamiento delictivo no está determinado de esta forma por factores ambientales, educativos, psicológicos o biológicos/antropológicos que inciden sobre un

<https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf> [Fecha de consulta: 20 de abril de 2022].

⁹¹ LABORATORIO DE INVESTIGACIÓN ESET (2021): *ESET Security Report (ESR) Latinoamérica 2021*. Disponible en: <https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf> [Fecha de consulta: 20 de abril de 2022].

⁹² EUROPOL (2021): *Internet Organised Crime Threat Assessment (IOCTA) 2021*, Publications Office of the European Union. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf [Fecha de consulta: 20 de abril de 2022].

⁹³ MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA (2020): *Informe sobre la Cibercriminalidad en España 2020*. Disponible en: <https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2020/INFORME-Cibercriminalidad-2020.pdf> [Fecha de consulta: 25 de noviembre de 2023].

⁹⁴ Esta teoría criminológica, cuyo enfoque se centra en la economía, bebe directamente de la teoría de la elección racional, también conocida como la teoría de la acción racional. La misma pertenece al marco teórico de la Ciencia Política y ha sido utilizada para entender y modelar el comportamiento económico. Los principales exponentes de esta teoría han sido Milton Friedman, Anthony Downs y Raymond Aron. Los críticos acérrimos de esta corriente han sido Amartya Sen y Mario Bunge.

individuo orillándolo a la comisión delictiva, sino por su propia elección basada en un análisis racional sobre los costos y los beneficios que implica delinquir.

Remitirnos a los conceptos de costo y beneficio rápidamente nos revela que esta teoría sobre el crimen posee un marcado enfoque economicista. Esta idea ha sido desarrollada en 1968 por Gary Becker⁹⁵ en un texto científico en donde abordaba esta noción sobre las elecciones racionales basadas en la relación costo-beneficio en un ámbito en donde la racionalidad a menudo se ha puesto en entredicho: la delincuencia. Esta estimación de los costes y beneficios que implica tener un comportamiento delictivo y de los costes y beneficios del comportamiento no delictivo como alternativa, actúan como una guía de estudio para la decisión de un sujeto. En consecuencia, la decisión de delinquir o no de una persona se basa en una ponderación estrictamente racional sobre estos dos tipos de costos y beneficios.

El anonimato es uno de los beneficios más valorados en el nodo que representa Internet. Con el anonimato desaparece el temor a ser identificado y, por consiguiente, el temor a ser detenido. Teniendo en cuenta que, según la teoría de la elección racional, un delincuente sopesa los riesgos potenciales en relación con los beneficios que proporciona un determinado acto delictivo, cabe considerar que el anonimato sea un parámetro con valoración positiva que tiende a inclinar la balanza hacia la conducta criminal.

El anonimato siempre dificulta la identificación. Al presente, la identificación de un cibercriminal que sabe cubrir su rastro en Internet resulta muy dificultosa o lenta, y requiere de unos tiempos puntuales de seguimiento e investigación, a fin de recabar los elementos que se acepten como medio de prueba en un juicio. En estos mismos términos judiciales probatorios cabe señalar que no basta únicamente con identificar la dirección IP de un ordenador, sino que debe de relacionarse dicho ordenador a un individuo concreto. Los actuales sistemas de identificación biométrica, la cibervigilancia, y la cooperación entre la esfera pública y privada tienden a eliminar o minimizar el sesgo de error de una incorrecta identificación, así como a acortar los tiempos de investigación y respuesta de las autoridades policiales.

Más allá de la relación establecida previamente con los tres enfoques teóricos de la oportunidad existen, sin lugar a duda, otras características inherentes a Internet como nuevo espacio de comisión delictiva.

Una de estas consideraciones está relacionada con el número significativo de crímenes que se comenten en Internet. Debido al hecho de que el agresor motivado y la víctima no se encuentran en el mismo espacio físico, la potencialidad del delito en el ciberespacio aumenta porque no se encuentra restringido a lo temporalmente cercano.

Ni la distancia física, ni la necesidad de un espacio común entre agresor y víctima actúan entonces como condicionantes de un evento criminal. Precisamente por la falta de esta corta distancia es que hay determinados crímenes que dejan de tener lugar, y ellos son aquellos que necesitan proximidad física como ser la violación o el asesinato. No obstante, aunque exista esta

⁹⁵ BECKER, Gary S. (1968) «Crime and Punishment: An Economic Approach», *Journal of Political Economy*, University of Chicago Press, Vol. 76, No. 2, pp. 169-217.

contracción con relación a la variedad de crímenes⁹⁶, existe a su vez una expansión en relación con el número de crímenes cometidos.

Otra de estas consideraciones está relacionada con el objetivo del delito. Es la víctima, en el caso de cualquier tipo de crimen cometido en Internet, quien decide cuál es el objeto de un potencial delito.⁹⁷ Es decir, son los propios usuarios de Internet quienes con sus conductas sobre el uso de la red exponen bienes jurídicamente protegidos, como pueden ser el patrimonio, la dignidad, la intimidad, etc. La decisión voluntaria de difundir en Internet cualquier bien jurídicamente protegido o cualquier información personal que pueda vulnerar estos bienes por terceros, sitúa a estos bienes como un objeto fácil de delito.

Un tercer elemento por considerar está vinculado con el factor tiempo, es decir, con el tiempo de permanencia de los elementos y/o acciones delictivas en el ciberespacio.

Según Miró Llinares, el ciberespacio puede convertir en perenne lo que en el espacio físico es instantáneo y caduco.⁹⁸ Este hecho acerca de la permanencia de un elemento o acción delictiva en Internet representa una diferencia sustancial respecto de los delitos que tienen lugar en un espacio físico real.

Internet permite una comisión y una concreción del delito en diferentes tiempos. En Internet el delito puede suceder hoy y hacer sentir sus efectos en el futuro. Por ello, se debe distinguir siempre en la red, la comisión respecto de la concreción del hecho delictivo.

Por un lado, existe la comisión del delito que tiene lugar cuando el agresor motivado lleva a cabo el delito en sí mismo; y por el otro, existe la concreción del delito y ello es cuando el delito cometido surte sus efectos en una o varias víctimas.

La existencia de Internet ha permitido que se desarrolle un tiempo asincrónico entre una y otra acción, de tal forma que el tiempo en el que se comete el delito no tiene por qué coincidir con el tiempo en el cual el delito se concreta para la víctima.

Si tenemos en consideración una línea de tiempo, podemos identificar el momento en el que se lleva a cabo la acción delictiva (tiempo presente), y el tiempo o los tiempos en lo que tiene lugar dichos efectos asincrónicos (tiempo 1, tiempo 2, etc.).

Existe, además, otro elemento de relevancia con relación a los tiempos de los delitos cometidos en Internet y ello es la permanencia indefinida de los delitos en la red. Llevar a cabo una acción delictiva en un tiempo presente, implica que ese delito perdure en el tiempo y que pueda ser replicado por otras personas de forma intencional, es decir con conocimiento del hecho delictivo realizado previamente; o por absoluto desconocimiento, simplemente por desconocimiento de la conducta delictiva. Estaríamos en este caso ante un efecto multiplicador del delito que se constituye, la gran mayoría de veces por mero desconocimiento del hecho delictivo o por ignorancia de las repercusiones legales.

⁹⁶ Cabe mencionar aquí que, si bien hay crímenes cuya comisión no tiene lugar en Internet debido a una limitación material, estos pueden ser sustituidos, desde un punto de vista cuantitativo, por los nuevos crímenes surgidos a la vera de esta nueva tecnología. Me refiero específicamente a los delitos tecnológicos o *high-tech crimes*.

⁹⁷ MIRÓ LLINARES, Fernando (2011), opus cit., pp. 1-55.

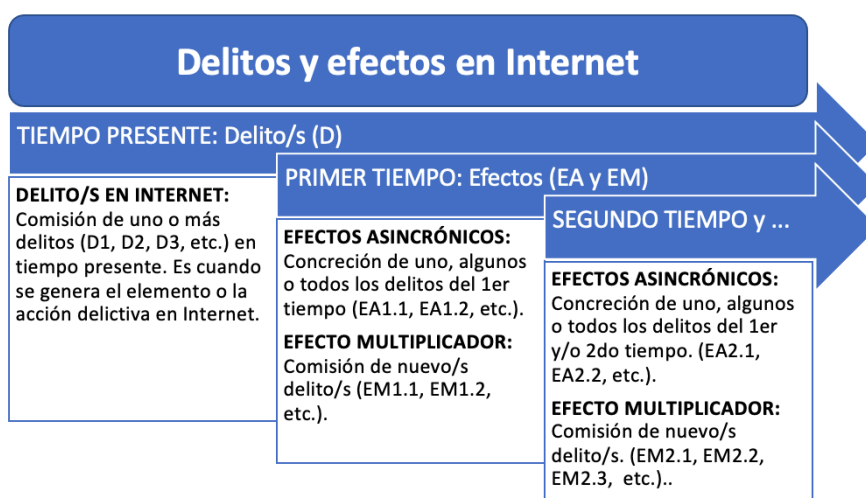
⁹⁸ *Ibidem*; p. 8.

Este tiempo asincrónico permite múltiples ecuaciones de concreción delictiva, por lo que genera un efecto multiplicador del delito en Internet.

Para ilustrar todo lo anterior consideremos el siguiente ejemplo: una persona publica en la red un link de descarga de un programa informático con el objeto de ofrecerlo de manera gratuita a los usuarios de Internet. Dicho programa contiene un virus troyano que le facilitará acceder remotamente a la información del ordenador que infecte. En el momento de la publicación de dicho link podemos identificar un hecho delictivo en tiempo presente. No obstante, supongamos la situación de que dicho programa no es descargado por ningún usuario, sino hasta dos meses después. Es decir, el link estuvo activo desde el hecho delictivo pero no cumplió sus efectos sino hasta tiempo después. En el momento en que una persona se descarga el programa, e infecta su ordenador se constituye como víctima de un delito y tiene lugar el tiempo primero, en donde suceden los efectos asincrónicos. Finalmente manteniéndonos en el mismo ejemplo, supongamos que una persona dueña de un blog de tecnología se encuentra en la red con este link que ofrece el programa de forma gratuita, y decide copiar y pegar el link en su blog para ofrecer a sus seguidores un programa gratuito. Sin saberlo, en este acto estaría estableciendo un efecto multiplicador del delito, y por tanto la concreción de nuevos hechos delictivos.

Este tiempo asincrónico entre el delito y sus efectos en Internet podría graficarse de la siguiente manera:

Gráfico 3: Relación asincrónica entre el delito en Internet y sus efectos.



Fuente: Elaboración propia. 2022.

Es preciso tener en cuenta que, tal como decíamos al inicio de este capítulo, Internet es primordialmente un lugar de comunicación y/o relación, en donde esta comunicación y/o relación no posee una naturaleza física y efímera, sino intangible y temporalmente indefinida. Aguirre Romero⁹⁹, sostiene que el ciberespacio es un espacio que solo surge a partir del intercambio de información en donde las personas que se encuentran y relacionan, generan una

⁹⁹ AGUIRRE ROMERO, Joaquín M. (2004): «Ciberespacio y comunicación: nuevas formas de vertebración social en el Siglo XXI», *Espéculo. Revista de estudios literarios (EREL)*, Universidad Complutense de Madrid, N.º 27, jul-oct.

red de interacción que posibilita su existencia. Según el autor, el ciberespacio agota su existencia en cuanto el mismo sirva para la comunicación entre los sujetos, dado que sin interacción no hay red. Esto plantea un concepto completamente opuesto al del espacio físico, dado que el mismo es anterior y posterior al individuo y a cualquier interacción de personas.

Comprender la naturaleza de Internet es fundamental para la luchar contra la criminalidad en este medio. Lo que resulta claro a priori en el análisis de este nuevo escenario que representa Internet es que su control y vigilancia requiere de un esfuerzo plural por parte de las instituciones nacionales, europeas e internacionales, y los usuarios de la red a nivel global.¹⁰⁰

¹⁰⁰ CANO PAÑOS, Miguel Ángel (2019a): «Criminalidad virtual: ¿Vino viejo en botellas nuevas? Traducción y nota previa de Miguel Ángel Cano Paños», *Revista Electrónica de Criminología*, 02-01, 1-8, p.4.

CAPÍTULO 3: EL USO YIHADISTA DE INTERNET Y LA E-YIHAD DEL AUTOPROCLAMADO ESTADO ISLAMICO

Hace más de diez años, concretamente en el año 2012, durante el 67 periodo de sesiones de la Asamblea General de las Naciones Unidas se adoptó una resolución relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. En esta resolución se expresaba “preocupación ante la posibilidad de que estas tecnologías y medios se utilicen con propósitos incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales y afecten negativamente a la integridad de la infraestructura” y, por ello, se instó tempranamente a los Estados a “impedir que los recursos o las tecnologías de la información se utilicen con fines delictivos o terroristas”.¹⁰¹

Hemos señalado, en el capítulo anterior, que uno de los elementos que promueve el aspecto transnacional de las acciones terroristas, es Internet. Las nuevas tecnologías han alcanzado tal alto grado de desarrollo que en la actualidad el impacto de la acción terrorista es global.

Este alcance sobre el uso de la red se ve primordialmente reflejado en dos segmentos: por un lado, el terrorismo yihadista dirige su mensaje a la ciudadanía global, incluyendo en este grupo a representantes de poderes públicos; y por el otro, orienta su mensaje a los simpatizantes, ocultos o manifiestos, del propio yihadismo. En el primer caso, el uso de la violencia (mediante la ejecución de atentados de propia autoría que luego son publicados en línea), o la amenaza del uso de la violencia (mediante la publicación en la red de alertas, comunicados o ultimátums) genera el mensaje indiscriminado y desestabilizador de terror en la sociedad. En el segundo caso, la búsqueda de simpatizantes externos (mediante publicaciones propagandísticas y segmentadas hacia diferentes públicos de interés) implica el desarrollo online de un discurso orientado a la captación de nuevos miembros. La puesta en práctica de estas dos líneas de actuación en Internet, llevadas a cabo por una organización yihadista, supone la ampliación de sus manifestaciones violentas y un alcance exponencial de su discurso ideológico.

Existen, sin embargo, otros usos de Internet con fines yihadistas, que atienden a una diversa especificidad de criterios, que establecen una clasificación vigente que facilita la comprensión del fenómeno y la persecución internacional.

Esta clasificación ha sido desarrollada en el año 2012 por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) quien elaboró un documento¹⁰², en colaboración con el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, en donde se describen los principales usos de Internet con fines terroristas.

La UNODC establece una clasificación de los usos de Internet por parte del terrorismo en seis categorías, siendo estas, 1. Propaganda (dentro de este apartado se encuentra incluida la propaganda con fines de reclutamiento, propaganda destinada a la incitación del terrorismo, y propaganda dirigida a la radicalización), 2. Financiación, 3. Adiestramiento, 4. Planificación (toma en consideración la utilización de comunicaciones secretas y la información de dominio público), 5. Ejecución y 6. Ataques cibernéticos.

¹⁰¹ Véase: UN A/RES/67/27, de 3 diciembre 2012.

¹⁰² UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012): *The use of the Internet for terrorist purposes*. New York: UNODC.

Cabe señalar que esta clasificación resulta fundamental como punto de partida para todas las acciones de contrterrorismo que se realizan al presente en el Sistema internacional con el fin de contrarrestar los efectos del yihadismo online.

A continuación, analizaremos la clasificación de la UNODC:

1. Propaganda

La propaganda representa uno de los principales usos que hacen los terroristas de Internet. Por medio de comunicaciones gráficas y/o audiovisuales se promueve y propaga el mensaje, ideología o acciones terroristas. El material consiste en mensajes contenidos en presentaciones, revistas, imágenes, videos, audios, juegos de video, etc. En este punto específico de la propaganda, la UNODC introduce un elemento de controversia conforme considera que debe diferenciarse aquello que es propaganda terrorista respecto de lo que denomina *promoción legítima*, aludiendo que “la propaganda en sí y de por sí no es una actividad prohibida”.¹⁰³ Aun ante esta distinción, entre propaganda legítima y no legítima, el documento de la UNODC recoge que “la promoción de la violencia es un tema común de la propaganda relacionada con el terrorismo.”¹⁰⁴

Para los grupos terroristas, la promoción de la violencia en Internet representa un elemento fundamental porque aumenta exponencialmente el volumen del público receptor. Las nuevas tecnologías de la información permiten controlar la creación y distribución del mensaje, sin que el contenido de este sea sometido a censura por parte de los medios de comunicación tradicionales. En adición a la promoción de imágenes violentas¹⁰⁵, se encuentra también la promoción de la retórica extremista que busca fomentar e incentivar los actos de violencia. Este contenido retórico es generado no solo por los grupos terroristas, sino también por simpatizantes de estos grupos y por medio de plataformas habituales de comunicación en Internet.

Conforme al documento elaborado por el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, la información propagandística pueden ser distribuida utilizando una amplia gama de instrumentos de las nuevas tecnologías de la información, tales como “sitios web especiales, salas virtuales de charlas y foros, revistas en línea, plataformas de redes sociales como *X* (ex *Twitter*) y *Facebook*, y sitios web populares de videos y de intercambio de ficheros como *YouTube* y *Rapidshare*, respectivamente.”¹⁰⁶ Esta retorica busca fomentar la propagación del mensaje de violencia extremista. Al respecto, Cano Paños afirma que, a diferencia de los foros privados, “en las redes sociales [por su carácter público] es

¹⁰³ Cabe señalar en este punto que, si bien la propaganda no es una actividad prohibida, si lo es el hecho de propagar mensajes cuyo fundamento básico sea la comisión de un delito o el fomento de la comisión de un delito. Es decir, se puede propagar la ideología (Por ej.: La interpretación espiritual del islam) sin que eso represente una actividad prohibida; o bien, se pueden propagar mensajes radicales (Por ej.: Acciones violentas del islam político) que representan actividades prohibidas de tipo delictivo.

En este punto, la UNODC introduce esta distinción conforme encuentra al primer tipo de propaganda un instrumento legítimo para el derecho a la libertad de expresión. No obstante, no debe olvidarse que siempre que se refiera al ‘uso de Internet con fines terroristas’ se tratará siempre de un uso cuya finalidad última es la comisión de un delito.

¹⁰⁴ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 4.

¹⁰⁵ Recurso frecuentemente utilizado por ISIS.

¹⁰⁶ *Ibidem*, p. 4-5.

relativamente sencillo observar la evolución de la propaganda, la ideología o la incitación a la violencia”, lo que facilita a su vez la persecución por medio de la vía penal.¹⁰⁷

La importancia de la propaganda terrorista en Internet, y asimismo su aspecto más peligroso, radica en que Internet permite llegar a todo tipo de usuario, simpatizante o no, por medio del uso común de servicios como *Instagram*, *Facebook*, *X* (ex *Twitter*), *WhatsApp*, *YouTube*, *TikTok*, *Tumblr*, Internet memes (ver: #catsofjihad) y otras redes sociales. No requiere necesariamente una posición activa del sujeto receptor,¹⁰⁸ como sucedía anteriormente en donde el interesado debía obtener la información mediante una búsqueda intencional. En el presente, la propaganda llega a todo tipo de público, transformando a cualquier usuario de Internet en posible sujeto receptor del mensaje¹⁰⁹. Esta propaganda puede centrarse en el reclutamiento, en la radicalización o en la incitación al terrorismo.

1.a. Reclutamiento

Aquellas personas que son receptivas a la propaganda terrorista (encausada bajo argumentos sobre fines nobles, la motivación política, la justificación de la violencia terrorista, fundamentos históricos o teológicos, etc.) suelen ser contactadas a fin de solicitarles apoyo. Las organizaciones terroristas utilizan en este caso la propaganda como antesala al reclutamiento clandestino. La idoneidad de Internet para esta actividad radica en su alcance y en su anonimato.¹¹⁰

La propaganda terrorista con fines de reclutamiento habitualmente se gesta con la intención de atraer sectores sociales vulnerables y marginales. “El proceso de reclutamiento y radicalización comúnmente explota los sentimientos de injusticia, exclusión o humillación, que en particular se tienen dentro de muchas comunidades musulmanas en Europa.”¹¹¹ Cabe señalar que “con frecuencia, estas percepciones y sensaciones son subestimadas desde la perspectiva occidental”¹¹², lo que ayuda a acrecentar el reclutamiento.¹¹³

Generalmente la propaganda destinada al reclutamiento se segmenta en los públicos a los que va dirigida,¹¹⁴ por tanto considera, entre otros factores, aspectos demográficos, situación socioeconómica, edad, género, idioma materno, etc. Esta segmentación no solo se manifiesta en el mensaje, sino también en el soporte escogido para contener el

¹⁰⁷ CANO PAÑOS, Miguel Ángel (2016): «Odio e incitación a la violencia en el contexto del terrorismo islamista. Internet como elemento ambiental», *Revista para el análisis del derecho In Dret*, 4/2016, p. 20.

¹⁰⁸ Esta afirmación se refiere al hecho de que los contenidos propagandísticos antes se distribuían a un público limitado conforme requería de la participación activa del sujeto para buscar y obtener la información en medios físicos (libros, CD, DVD, etc.). Este sujeto activo era a priori siempre un sujeto interesado en la información conforme la buscaba intencionalmente.

¹⁰⁹ El mensaje propagandístico de los grupos terroristas suele contener amenazas de violencia o imágenes de actos de violencia aunado al espíritu de orgullo, no obstante, “con respecto a la comunidad internacional en general, el objetivo es a menudo transmitir el deseo de lograr nobles fines políticos.” UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 5.

¹¹⁰ “El alcance de Internet proporciona a las organizaciones terroristas simpatizantes un semillero mundial de reclutas potenciales.” [...] “El uso de barreras tecnológicas al acceso a las plataformas de reclutamiento también aumenta la complejidad del rastreo de las actividades relacionadas con el terrorismo por los agentes de los servicios de inteligencia y las fuerzas del orden.” *Ibidem*.

¹¹¹ EUROPEAN COMMISSION'S EXPERT GROUP ON VIOLENT RADICALISATION (2008), opus cit., p. 9.

¹¹² *Ibidem*.

¹¹³ Muchos usuarios en esta situación encuentran en Internet un ‘refugio virtual’ acrecentado en el hecho de que el mensaje terrorista en la red es un mensaje más relajado, idealizado, superficial, pero también más visual.

¹¹⁴ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 5-6

mismo¹¹⁵. Adicionalmente, el mensaje suele estar signado por la idealización, la belleza, la nobleza, y la felicidad de la causa, buscando banalizar el mensaje de odio y violencia.¹¹⁶

Es importante destacar que existen numerosos casos de reclutamiento en Europa por medio de las nuevas tecnologías, el caso de las jóvenes ceutíes en España¹¹⁷ o el de Eric Breininger¹¹⁸ representan un ejemplo significativo de este hecho.

1.b. Incitación al terrorismo

Como se mencionó anteriormente, la propaganda no está prohibida. Sin embargo, en algunos Estados se considera ilegal el uso de la propaganda cuya finalidad sea cometer actos de terrorismo.

La inmensa mayoría del material propagandístico que promueve la incitación al terrorismo en Internet centra su mensaje en la glorificación de los actos terroristas cometidos o por cometer. La incitación al terrorismo busca alentar la comisión de estos delitos sin, necesariamente, ser un actor participe del acto terrorista. Internet, mediante una gran variedad de foros, páginas webs, redes sociales, blogs, etc., facilita la comunicación entre simpatizantes del terrorismo yihadista y facilita la incitación mediante la glorificación de los atentados o de los autores de estos.

1.c. Radicalización

En relación con el uso propagandístico de Internet por parte de los grupos terroristas puede considerarse a la radicalización como el último estadio de la promoción de la propaganda.

Conforme a lo recogido en el Capítulo I del Informe de la UNODC “La radicalización se refiere principalmente al proceso de adoctrinamiento que suele acompañar a la transformación de los reclutas en personas decididas a actuar con violencia, inspiradas por ideologías extremistas.”¹¹⁹

La radicalización es un proceso que debe ir acompañado de mensajes continuados, y segmentados en el propósito del hecho que se pretende conseguir y en las particularidades del sujeto a quien va dirigido. “Una mención especial dentro de los

¹¹⁵ En el reclutamiento de menores se utilizan habitualmente mensajes contenidos en dibujos animados, canciones, cuentos infantiles, videos de música popular o juegos de computadora, que glorifican actos de terrorismo, como, por ejemplo, los atentados suicidas. WEIMANN, Gabriel (2008): «Online terrorist prey on the vulnerable», *YaleGlobal Online*. Disponible en: <https://archive-yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable> [Fecha de consulta: 23 noviembre 2023].

¹¹⁶ Tales características se aprecian en la película de ISIS, *Eid Greetings from the Land of Khilafah* (Saludos desde la tierra del califato), filmada en Siria, cuya temática se centra en mostrar como un sueño hecho realidad diferentes viajes de enrolamiento yihadista desde Finlandia, Reino Unido, Marruecos, Indonesia, etc.

¹¹⁷ Particularmente relevante fue el caso de Aicha (Ceuta, España) de 14 años, primer caso de una menor española enrolada en la yihad por medio de la red, en octubre de 2014. Reclutada en redes sociales por medio del teléfono móvil.

¹¹⁸ En este caso “la publicación y a buen seguro meteórica difusión a través de Internet de las memorias del joven alemán converso ponen de relieve el papel trascendental que la red global de comunicaciones está jugando a la hora de impulsar y fortalecer los mecanismos de propaganda, adoctrinamiento y reclutamiento yihadista.” Véase: CANO PAÑOS, Miguel Ángel (2011): «Reflexiones y experiencias desde las entrañas del yihadismo militante. Análisis de la autobiografía de Eric Breininger», *UNISCI Discussion Papers*, (26), mayo de 2011, p. 221.

¹¹⁹ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 7.

lugares proclives a la radicalización yihadista merece el caso de la red global de Internet como centro virtual de propagación del islamismo radical y la yihad.”¹²⁰

2. Financiación

Otros de los usos que suelen realizar de Internet los grupos terroristas es el vinculado a la financiación del terrorismo.

Conforme a la UNODC¹²¹, la forma en la que los terroristas utilizan Internet para la recaudación de fondos se puede dividir en cuatro categorías generales, estas son, la recaudación directa, el comercio electrónico, el empleo de los servicios de pago en línea y las contribuciones a organizaciones benéficas.

La recaudación directa se lleva a cabo utilizando los sitios web y las salas de charla, las campañas masivas de correo y las comunicaciones personalizadas dirigidas a simpatizantes para solicitar donaciones.

El comercio electrónico implica la creación de diferentes tiendas en línea que ofrecen de forma permanente productos digitales tales como e-books, audio, video u otros artículos descargables que resulten de interés de los simpatizantes.

Los servicios de pago en línea que ofrecen algunos sitios web o plataformas de comunicación especiales¹²² permiten la transferencia electrónica de fondos entre las partes. En el caso de los pagos en línea se debe tener presente que estas plataformas también pueden ser usadas mediante medios obtenidos de forma fraudulenta, como es el caso de las tarjetas de crédito robadas, el robo de identidad, etc. Las ganancias ilícitas obtenidas se utilizan para financiar los actos de terrorismo.¹²³ Los beneficios económicos obtenidos por medio del robo de tarjetas, habitualmente se blanquean por varios medios, entre ellos el pago en línea por e-Gold.¹²⁴

Finalmente encontramos las contribuciones a organizaciones benéficas. Habitualmente se trata de organizaciones en apariencia con fines legítimos y filantrópicos que dicen apoyar a causas sociales, humanitarias, etc.¹²⁵

3. Adiestramiento

Para las organizaciones terroristas, Internet representa un campo de adiestramiento alternativo. En la actualidad se pueden encontrar en línea numerosos manuales de entrenamiento en operaciones terroristas¹²⁶, y archivos de audio y video orientados a la

¹²⁰ CANO PAÑOS, Miguel Ángel (2008), opus cit., p. 75.

¹²¹ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 7-9.

¹²² Por ejemplo, la utilización de la transferencia bancaria electrónica, de la tarjeta de crédito o de servicios de pago alternativos ofrecidos por *PayPal* y *Skype*.

¹²³ Un ejemplo de ello es el caso de Reino Unido contra Tsouli y otros, referido a tres acusados que mantenían en activo unos 180 sitios web en donde se distribuía material ideológico extremista y manuales sobre armas y explosivos. El costo de mantenimiento de estos sitios de Internet y el apoyo a otras operaciones se sufragaba con el uso fraudulento de tarjetas de crédito robadas. Al momento de formularse los cargos, el fraude ascendía a 1,8 millones de libras esterlinas. Véase: R c. Tsouli y otros. [2007] EWCA (Crim) 3300.

¹²⁴ Moneda virtual cuya principal característica radica en que los fondos transferidos mediante tarjeta de crédito a este sistema automáticamente se convierten en oro, es decir son respaldados por oro físico. Se considera un sistema seguro en cuanto, una vez realizada la transferencia, no permite cancelar el pago. Y el dinero, una vez que ingresa en cuenta, no puede ser reclamado a la compañía. Otra de las características es que no requiere verificaciones, por lo tanto permite las operaciones económicas de forma anónima.

¹²⁵ *Benevolence International Foundation, Global Relief Foundation, y Holy Land Foundation for Relief and Development.*

¹²⁶ En ellos, por ejemplo, se enseña mediante tutoriales, cómo fabricar explosivos o armas de fuego, como manipular materiales peligrosos o cómo planear y ejecutar actos terroristas.

información táctica y estratégica. Estas páginas web actúan como verdaderos campos de entrenamiento virtual.¹²⁷

Adicionalmente a la información referida a las operaciones de adiestramiento, en estas páginas se suele poner a disposición del usuario métodos de afiliación a organizaciones terroristas. Asimismo, estas plataformas poseen foros en donde los usuarios pueden recibir información y mutuo asesoramiento, fomentada dicha actividad en el carácter anónimo, cifrado y comunitario de las comunicaciones.

4. Planificación

El mantenimiento de operaciones y actividades terroristas implica necesariamente el uso de la planificación. “En particular, la planificación de un acto de terrorismo típicamente implica la comunicación a distancia entre las partes”.¹²⁸ Y la comunicación a distancia solo es posible establecerla por medio de Internet.

Este uso de Internet, centrado exclusivamente en la planificación, es posible observarlo con claridad en el caso francés, Ministerio público c. Hicheur.¹²⁹ Este caso ilustra el uso de Internet para el sostenimiento de comunicaciones permanentes tendientes a planificar un atentado y la creación de una unidad de operación de Al Qaeda en el Magreb Islámico (AQMI), en Europa.

Con independencia de este caso, en términos generales Internet resulta un instrumento idóneo para el establecimiento de comunicaciones tendientes a la planificación de actividades terroristas.

Esta planificación adquiere dos modalidades: por medio de comunicaciones secretas y por medio de información de dominio público.

4.1 Por medio de comunicaciones secretas

Internet facilita la comunicación entre las partes del grupo terrorista. Al presente, gran número de personas que integran grupos terroristas poseen altos conocimientos en tecnologías de la información, de tal forma que permiten el acceso a niveles de Internet subterráneos en donde resulta más difícil rastrear los datos de usuario y registros de IP. También poseen conocimiento suficiente para establecer plataformas cerradas con sistema de encriptado.¹³⁰ Estos softwares de encriptado y anonimato pueden ser también fácilmente descargados de Internet, y permiten enmascarar IP, redirigir ubicaciones de ordenadores a otros servidores, etc.

Sin embargo, existe un sistema de comunicación secreta mucho más extendido entre todos los miembros de grupos terroristas, el cual consiste en el uso del correo electrónico ordinario y la utilización de drafts o borradores. Un proveedor de mail permite un registro gratuito sin verificación de identidad. El usuario creado y la contraseña son

¹²⁷ Por ejemplo, la revista online *Inspire* vinculada a Al Qaeda contenía en la edición de 2010 “material didáctico práctico sobre como adaptar un vehículo de tracción en las cuatro ruedas para llevar a cabo un ataque contra miembros del público [...]”. Véase: UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 9.

¹²⁸ *Ibidem*.

¹²⁹ Sentencia de 4 de mayo de 2012, causa núm. 0926639036 del Tribunal de Grande Instance de Paris (14ª Cámara/2), Paris.

¹³⁰ TUNG, Liam (2008): *Jihadists get World-class encryption kit*. Disponible en: www.zdnet.com.au/jihadist-get-world-class-encryption-kit-339285480.htm [Fecha de consulta: 21 de septiembre de 2020].

distribuidos entre los diferentes miembros con los que se quiere mantener comunicación. Mediante la creación y modificación de un borrador de correo electrónico los miembros se comunican accediendo a dicha cuenta de correo y a dicho borrador desde diferentes partes del mundo. El borrador del correo electrónico jamás se envía para que no ingrese la información que el mismo contiene al circuito “visible” de comunicaciones en Internet. Es decir, mientras que un borrador de correo electrónico no sea enviado como un correo electrónico habitual, es prácticamente imposible de rastrear para los sistemas de inteligencia contra el terrorismo. Esto facilita la comunicación interna entre las partes manteniendo altos niveles de privacidad. Ello resulta especialmente útil en casos como el empleo de la *Hawala*¹³¹.

4.2 Por medio de la información de dominio público

El uso de la información de dominio público tiene dos sentidos: creación y consumo. Como creadores de información, los grupos terroristas publican en Internet gran cantidad de contenido de acceso libre, ello con el objeto de potenciar su mensaje y la interacción con el público.

Por otra parte, el consumo de información de dominio público es lo que les permite llevar adelante hechos ilícitos con precisión en cuanto incorporan a la planificación datos concretos tales como horarios de transporte, planos de aviones y edificios públicos, información de materiales constructivos de ciertos medios de transporte, el uso de Google Earth, de sistemas de ventilación de metros, de distribución de una ciudad, etc. Múltiple información que diferentes empresas, organismos públicos, proveedores de servicios, e incluso particulares ponen a disposición del usuario para fines legítimos, pueden ser utilizados como información de logística detallada.

Este aspecto es particularmente relevante en cuanto está teniendo lugar en una era en donde la presencia web de las empresas, de las instituciones, de los gobiernos, de las personas, parece inexcusable. Todo resulta susceptible de ser publicado en Internet y esa información, una vez en Internet, puede terminar siendo usada para diversos usos y hechos ilícitos.

5. Ejecución

El uso de Internet en el ámbito de la ejecución implica la amenaza explícita de violencia. Suele utilizarse la red para dar a conocer las intenciones del grupo terrorista de llevar a cabo un potencial acto terrorista con el objeto de generar ansiedad o miedo en la población.

También se suele utilizar bajo una manifiesta intención de chantaje o extorsión en donde ante la amenaza de realizar alguna acción o no realizarla, se busca transmitir temor y generar influencia política. Un claro ejemplo de esto es aquel que ilustra el amplio uso que se hizo de la red meses antes de la perpetración del atentado en Estados Unidos llevado a cabo el 11

¹³¹ *Hawala* significa ‘transferencia o cable’ en árabe. Es un sistema de intercambio de divisas que tiene siglos de historia, y consiste en realizar un transferencia monetaria informal cuando, por algún motivo concreto -inmigración irregular, no tendencia de identificación oficial, pedido de captura, etc.-, una persona no puede acceder al sistema bancario de un lugar determinado. Implica una transferencia de fondos de un lugar a otro y se basa en la confianza de intermediarios conocidos como hawaladars. Por la naturaleza de sus comunicaciones privadas es un sistema de transferencias que casi no deja rastro.

de septiembre de 2001, en donde se alertaba en numerosas páginas web y foros no yihadistas de un ataque inminente a un objetivo estadounidense.¹³²

Además de facilitar la amenaza, “para la ejecución de actos terroristas Internet puede, entre otras cosas, ofrecer ventajas logísticas, reducir las probabilidades de detección y encubrir la identidad de responsables”¹³³

6. Ataques cibernéticos

Un ciberataque se refiere al ataque deliberado de una o varias páginas web, servidores web, sistemas de redes, etc. “Estos ataques suelen estar destinados a perturbar el funcionamiento normal de los blancos elegidos” ... “mediante técnicas de piratería informática, virus informáticos, programas maliciosos, *phlooding* o cualquier otro medio de acceso no autorizado”¹³⁴ Los ciberataques poseen todas las características de un acto de terrorismo, por dicho motivo se hace referencia a esta práctica como *ciberterrorismo*.

En la última década, los grupos terroristas han comenzado a utilizar las Tecnologías de la Información y Comunicación (TIC) para la perpetración de las propias acciones terroristas, sustituyendo en parte los objetivos de ataque habituales por objetivos vinculados a la información. El ciberterrorismo comprende de este modo un nuevo campo físico de acción de las acciones terroristas. Es decir, implica un desplazamiento de un conflicto previo.

Según Orta Martínez, el ciberterrorismo es la convergencia del ciberespacio y el terrorismo. Se refiere a ataques ilegales y amenazas de ataques contra computadoras, redes y la información almacenada en ellas, cuando son llevados a cabo para intimidar o forzar a un gobierno o a su pueblo en la búsqueda de objetivos políticos y sociales.¹³⁵

La posibilidad de utilizar Internet por parte de grupos terroristas es muy amplia. Internet posee múltiples características que favorecen las acciones de los grupos terroristas para perpetrar ataques. La red, asimismo, permite coordinar y planificar operaciones muy dispares, desde la planeación y financiación hasta la radicalización o difusión global de un virus.

Conforme a Miró Llinares “Las TIC, en general, e Internet como red global, en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que ha sido denominado ‘El Ciberespacio’, y respecto al cual nos debemos plantear si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o, por el contrario, idéntico a este en sus caracteres esenciales.”¹³⁶

El citado informe de la UNODC nace de la creciente amenaza del terrorismo y de la necesidad de detallar sus acciones en un nuevo marco de acción. Esta creciente preocupación deriva de las numerosas y actuales actividades con finalidad delictiva que el terrorismo realiza valiéndose de Internet como un nuevo instrumento de operación. No obstante, aun cuando en los últimos años se viene reconociendo cada vez más la amenaza que representa el uso de Internet por las

¹³² WEIMANN, Gabriel (2004): «Terrorismo e internet», *Revista Ética Net*, (3), p. 4.

¹³³ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 12.

¹³⁴ *Ibidem*.

¹³⁵ ORTA MARTÍNEZ, Raymond (2005): «Ciberterrorismo», *Alfa Redi, Derecho y Nuevas Tecnologías* (82). Disponible en: <http://www.alfa-redi.org/node/9537> [Fecha de consulta: 21 de septiembre de 2020].

¹³⁶ MIRÓ LLINARES, Fernando (2011), opus cit., p. 4.

organizaciones y grupos terroristas, actualmente no existe ningún instrumento universal que se refiera puntualmente a este tipo de modalidad delictiva por parte de los terroristas. Paralelamente, el informe reconoce que hay pocos programas de capacitación especializada en los aspectos jurídicos y prácticos de la investigación y el enjuiciamiento de casos de terrorismo en que se haya usado Internet.¹³⁷

A continuación, y a fin de sintetizar toda la información anteriormente presentada, se ordenan en una tabla los principales usos de Internet por parte de grupos los terroristas, detallando el uso habitual de la red, la finalidad que posee dicho uso, un ejemplo ilustrativo de cada utilización y el tipo delictivo que representa cada uso de Internet descrito de acuerdo con la normativa internacional, la normativa europea, y la normativa de España como caso específico de un país miembro de la UE.

Cabe señalar que las medidas normativas que se enuncian en la siguiente tabla se analizarán en profundidad y en conjunto a las medidas institucionales de cooperación y las medidas preventivas, en la segunda parte de esta investigación al abordar la Política Criminal. Se considera no obstante pertinente el enunciar la normativa en esta tipología a fin de que sea una aproximación al tema, pero bajo ningún aspecto agota su análisis.

Tabla 1. Tipología sobre los usos de Internet de los grupos terroristas y su tipo delictivo en la UE y España.

USO	FINALIDAD	EJEMPLO/s	TIPO DELICTIVO
PROPAGANDA (RECLUTAMIENTO) Uso de correo electrónico, foros y redes sociales y otros medios de comunicación online.	Captación de nuevos miembros, comunicación entre diferentes células, coordinación de acciones.	Comunicados del Comité Militar de Al Qaeda en la Península Arábiga para reclutar suicidas mediante foros de Internet yihadistas.	Captación de terroristas Recogido: - En el Derecho Internacional en: <i>Art. 5.1.a. de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional</i> - En la legislación de la UE: <i>Art. 3.1.b Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 577.2 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. (doctrinamiento activo).</i>

¹³⁷ La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) sostiene que “El uso de Internet con fines terroristas es un fenómeno que se propaga con rapidez y exige una respuesta dinámica y coordinada de los Estados Miembros. [...] En 2011, la Asamblea General, en su resolución 66/178, reafirmó el mandato de la UNODC de seguir desarrollando los conocimientos jurídicos especializados en el campo de la lucha contra el terrorismo y en las esferas temáticas pertinentes, incluido el uso de Internet con fines terroristas.” Véase: ORTA MARTÍNEZ, Raymond (2005), opus cit. Disponible en: <http://www.alfa-redi.org/node/9537>; p. v. [Fecha de consulta: 21 de septiembre de 2020].

PROPAGANDA (INCITACIÓN AL TERRORISMO) Publicación, en foros y redes sociales, de mensajes que elogien o celebren actos terroristas perpetrados por sí mismos y/o por otros grupos terroristas. Publicación, en foros y redes sociales, de mensajes que inciten a la comisión de actos terroristas.	Legitimación del método, difusión de ideología, propaganda, terror.	Después del 11-M en España, en una mezquita cerca de la Alhambra se vendían CD's de 'propaganda islamista' que celebraba la comisión del atentado y hacia un amplio llamamiento a la comisión de nuevos actos. Dichos CD's contenían información recogida de Internet. ¹³⁸	Incitación al terrorismo. Recogido: - En Derecho Internacional en: <i>UN A/RES/1373 (2001)</i> . - En la legislación de la UE: <i>Art. 3.1.a Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 578 (enaltecimiento) 579 (incitación) Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.</i>
PROPAGANDA (RADICALIZACIÓN) Mensajes continuados, y segmentados de adoctrinamiento.	Convicción para la actuación con violencia extrema para la comisión de actos.	Videos de ejecuciones de Al Qaeda o de Daesh publicados en YouTube.	Radicalización Recogido: - En el Derecho Internacional en: <i>Convenio Internacional para la represión de la financiación del terrorismo (1999)</i> . - En la legislación de la UE: <i>Art. 3.1.c Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 577.2 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. (adoctrinamiento activo).</i>
FINANCIACIÓN Uso del sistema electrónico bancario y medios alternativos de pago. Uso fraudulento de tarjetas de crédito en plataformas online.	Obtención de fondos para el soporte de operaciones.	Caso R c. Tsouli y otros. [2007] EWCA (Crim) 3300.	Financiación del terrorismo. Recogido: - En el Derecho Internacional en: <i>Convenio Internacional para la represión de la financiación del terrorismo (1999)</i> . - En la legislación de la UE: <i>Directiva del Consejo número 91/308/EEC.</i> - En normativa interna (España): <i>Art. 576 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.</i>

¹³⁸ REINARES, Fernando (2005), opus cit., p. 5.

ADIESTRAMIENTO Publicación de manuales y documentos con contenido, ideología y principios de la acción terrorista.	Adoctrinamiento, instrucción armamentística y religiosa.	Manuales online: “Manual de venenos de los muyahidines”, “El Manual de la Yihad Afgana”, “Manual de Al Qaeda”, “Los secretos de los muyahidines”, o consejos sobre atentados terroristas publicados en la revista online <i>Inspire</i> de Al Qaeda, y en la desaparecida revista <i>Rumiyah</i> o <i>Dabiq</i> del Estado Islámico.	Adoctrinamiento. Recogido: - En el Derecho Internacional en: <i>UN A/RES/1373 (2001)</i> . - En la legislación de la UE: <i>Art. 3.1.c Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 575.2 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. (adoctrinamiento pasivo).</i>
PLANIFICACIÓN (COMUNICACIONES SECRETAS) Uso de ‘borradores’ en el correo electrónico (<i>drafts</i>).	Coordinación y planificación segura de acciones.	Transferencia informal de fondos (TIF). (<i>Hawala</i>). ¹³⁹	Tentativa. Recogido: - En el Derecho Internacional en: <i>UN A/RES/1373 (2001)</i> . - En la legislación de la UE: <i>Art. 4.3 Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 577.1 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.</i>
PLANIFICACIÓN (INFORMACIÓN DE DOMINIO PÚBLICO) Obtención de información pública para logística detallada.	Eficacia de los ataques terroristas.	Imágenes satelitales mediante <i>Google Earth</i> .	Tentativa. Recogido: - En el Derecho Internacional en: <i>UN A/RES/1373 (2001)</i> . - En la legislación de la UE: <i>Art. 4.3 Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): <i>Art. 577.1 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.</i>
EJECUCIÓN Publicación, en foros y redes sociales, de mensajes que involucren amenazas de ejecución de futuros atentados.	Amenazas, manipulación, publicidad, terror, detentación de poder.	Mensajes recogidos en la web previos a los ataques del 11/9 a las Torres Gemelas, en los que Al Qaeda advertía de un “ataque eminente y a gran	Amenaza/Extorsión Recogido: - En el Derecho Internacional en: <i>Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.</i> - En la legislación de la UE: <i>Art. 3.2 e Decisión Marco 2008/919/JAI del</i>

¹³⁹ Véase: Reglamento de Ejecución (UE) N.º 261/2013 del Consejo de 21 de marzo de 2013.

		escala” a Estados Unidos. ¹⁴⁰	<i>Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo.</i> - En normativa interna (España): Art. 573 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.
ATAQUES CIBERNÉTICOS Piratería informática, virus informáticos, programas maliciosos, phlooding	Manipulación, detentación de poder.	Ciberataque a Israel (año 2012): implicó el ataque programado a múltiples objetivos estratégicos y simbólicos como la Bolsa de Valores de Tel Aviv, la compañía aérea nacional, y a diversos ciudadanos israelíes.	Delito informático. Recogido: - En el Derecho Internacional en: <i>Convenio sobre la Ciberdelincuencia, Serie de Tratados N.º 185, de 23 de noviembre de 2001. (Consejo de Europa).</i> - En la legislación de la UE: Art. 3.1.c Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo. - En normativa interna (España): Art. 573 Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

Fuente: Elaboración propia con base en la clasificación sobre el uso terrorista de Internet de la UNODC. 2020.

Habiendo determinado cuáles son los usos de Internet que realizan las organizaciones terroristas y esquematizados estos en una tipología que identifica los tipos delictivos que cada uso implica, lo siguiente es mencionar que de todos estos usos señalados, el uso de Internet cuya finalidad es la propaganda, ocupa un espacio de especial importancia.

La propaganda terrorista online ha ocupado gran parte de las actividades del yihadismo en los últimos años debido principalmente a que ha permitido un crecimiento sin precedentes del número de miembros de la organización, y a su vez ha facilitado las acciones de radicalización a distancia sobre cada simpatizante.

Habida cuenta de lo reseñado en el capítulo previo, en donde se pone de manifiesto la relevancia actual que posee Internet como nueva tecnología para la transmisión de mensajes, podemos esperar que las organizaciones terroristas actúen como cualquier otra organización y adhieran su cometido a esta evolución tecnológica, a fin de crear y difundir su ideología de forma exponencial.

El uso de las nuevas tecnologías por parte del terrorismo ha trascendido el mero hecho instrumental y se ha convertido en un proceso comunicativo propio. Los grupos terroristas comunican con intención. Esa intención comunicativa, de enfoque propagandista, se orienta hacia fines muy específicos y diversos como pueden ser el reclutamiento de simpatizantes, la radicalización de sus miembros, la legitimación internacional, infundir terror global, vanagloriar la yihad, desarrollar fundamentos teológicos para justificar el uso de la violencia, etc.

¹⁴⁰ WEIMANN, Gabriel (2004), opus cit., p. 3.

Es importante puntualizar que en el desarrollo de esta investigación no se desvalorizan otros usos, como el uso operativo, que realizan los grupos yihadistas de Internet. Por el contrario, se entiende que la utilización de la red resulta fundamental para la propia logística que implica toda acción terrorista, así como para la comunicación interna fluida que garantiza la pervivencia de la propia organización. No obstante, es preciso señalar que, salvo en contadas excepciones¹⁴¹, el avance tecnológico no ha supuesto un cambio radical en las acciones terroristas. Ha significado indudablemente una mejora instrumental pero no ha implicado un cambio sustancial que actúe como un parteaguas para el terrorismo internacional.

Por el contrario, el uso de Internet con fines propagandísticos ha significado una bisagra en la historia de las organizaciones terroristas globales, dado que ha magnificado la capacidad comunicativa de dichas organizaciones y ha lanzado con eficacia el nacimiento de su poder blando hacia dentro del Sistema internacional.

Según Joseph Nye, el Poder blando (o *Soft power*) se define como la capacidad de influencia que posee un actor (por ej., un Estado) sobre otro actor (por ej., otro Estado, una OO.II., etc.) dentro del Sistema internacional. Esta relación no se basa en premisas normativas, sino en condicionamientos u orientaciones persuasivas tendientes a garantizar los intereses propios dentro del sistema, valiéndose para ello de medios culturales, ideológicos, comunicativos, educativos, etc. En *Soft Power: The Means to Success in World Politics*, Nye afirma que “la seducción es más efectiva que la coacción, y [que] valores como la democracia, derechos humanos y oportunidades individuales son profundamente seductores”.¹⁴² Es precisamente el uso de Internet que realizan las organizaciones terroristas lo que determina el nacimiento y desarrollo de este poder.

A partir de este autoconocimiento del propio poder, las organizaciones terroristas inician el desarrollo de un elevado estatus comunicativo y comienzan a influir en el Sistema internacional, y lo hacen en última instancia mediante las oportunidades individuales a las que Nye hace referencia, ofertando en Internet a cada individuo del planeta la posibilidad de ser parte de la organización, ya sea como receptor y/o vocero de la narrativa yihadista, así también como un actor individual (*lobo solitario*) de atentados.

Las nuevas tecnologías han facilitado la creación del escaparate del terrorismo en donde se exponen mensajes propagandísticos dirigidos a los fines ya descritos¹⁴³, con una asiduidad cada vez mayor. Son estas acciones y este escaparate virtual lo que permite a estas organizaciones terroristas acumular poder. De ello deriva la importancia de las nuevas tecnologías para la yihad, dado que no se trata solo de una herramienta de utilización propagandística, sino de una herramienta de construcción de poder en el nuevo espacio público que representa el ciberespacio.

Con relación a ello, Lesaca ha señalado, que

«en la última década, [...], se ha acelerado un cambio estructural en el ámbito de la comunicación pública. Esta vez no se trata de una evolución tecnológica de los medios de comunicación, sino de un proceso que trasciende y supera a los propios medios. La evolución tecnológica generada por las redes sociales, la

¹⁴¹ Nos referimos aquí a acciones de ciberterrorismo, cuyo objetivo sea únicamente el ataque a sistemas informáticos.

¹⁴² NYE, Joseph. (2004): *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

¹⁴³ Léase (según la clasificación de UNODC): 1.a Reclutamiento, 1.b Incitación al terrorismo, y 1.c Radicalización.

democratización de los dispositivos móviles inteligentes y los aparatos electrónicos de grabación y edición de imagen y video en alta calidad han alterado los esquemas habituales de construcción de la opinión pública. Los medios tradicionales han perdido el monopolio que tenían asignado en este proceso, y su papel como mediadores entre los actores del proceso de comunicación ha quedado mermado. Los responsables del aparato de comunicación terrorista son muy conscientes del nuevo contexto y adaptan su estrategia de terror a la nueva realidad.»¹⁴⁴

Esta nueva conciencia acerca de su propio poder ha despertado en las organizaciones yihadistas a partir de la evolución tecnológica de la última década, y ha permitido la creación de un aparato comunicativo sin precedente: la e-yihad.

La e-yihad o la yihad online hace referencia a la conquista que han hecho las organizaciones terroristas de Internet. Nos referimos específicamente al desarrollo estratégico de una agenda ideológica y la implementación de múltiples actividades comunicativas en el ciberespacio, con la clara finalidad de establecer una narrativa propagandística.

Dentro de todos los grupos yihadistas que operan de forma global en la actualidad, es destacable el desempeño del autoproclamado Estado Islámico (EI).¹⁴⁵ Esta organización es relevante porque, dentro de todas las existentes, es aquella que supo capitalizar con creces el uso de Internet hacia los objetivos propagandísticos descritos previamente, y por ello puede sin lugar a duda ser reconocida como la precursora de la e-yihad.

En la actualidad, el EI posee un importante dominio de las nuevas tecnologías y un altísimo entendimiento de la comunicación audiovisual. En su gestión comunicativa, el aunar de ambas cualidades le ha otorgado una característica inigualable de ser la organización terrorista que destaca entre otras por su gran dotación de narrativa online.

No en vano el EI cuenta con la productora *Al Hayat*, el gigante mediático del grupo terrorista, un gran productor de propaganda para Internet que crea su contenido orientado a diferentes segmentos de audiencias, y en más de media docena de idiomas diferentes. Según Barrancos, “la gente que se une a ellos, sobre todo la que procede de Europa, tiene sus carreras universitarias, hay gente que sabe de cine, hay gente que sabe de fotografía...”.¹⁴⁶ Esta profesionalización de la comunicación dentro del Estado Islámico otorga, con relación a otros grupos terroristas, una enorme capacidad diferencial. Esta capacidad está orientada, como tantas otras, hacia los objetivos de propaganda en los cuales prevalece el reclutamiento de

¹⁴⁴ LESACA, Javier (2017): *Armas de seducción masiva*, Barcelona: Ediciones península, pp. 29-30.

¹⁴⁵ Debido a que se conoce con variedad de denominaciones, es pertinente mencionar que el nombre que se utilizará en esta investigación de este grupo terrorista es el de Estado Islámico de Irak y el Levante, cuyas siglas son EIIL (ISIL, en el mundo anglosajón, por *Islamic State of Iraq and the Levant*). Este nombre resulta una mejor opción que Estado Islámico de Irak y Siria (ISIS por *Islamic State of Iraq and Syria*) que también es utilizado en medios de comunicación de habla castellana e inglesa, ya que este último nombre no hace referencia a la Siria actual (República Árabe Siria), sino a la región de la Siria histórica que en español se conoce tradicionalmente como Levante. Por último, es pertinente mencionar que Dáesh (acrónimo árabe de *al-Dawla al-Islamiya al-Iraq al-Sham*, cuya traducción significa Estado Islámico de Irak y el Levante) es otra denominación muy utilizada por gobiernos anglosajones para referirse a este grupo terrorista. En árabe, el sonido de esa palabra es parecido a “algo que aplastar o pisotear”, y según como se conjugue, esta palabra también puede significar “intolerante” o “el que siembra la discordia”. Los miembros de la organización terrorista no solo rechazan esta denominación, sino que aplican la pena de muerte a cualquier persona que la utilice en los territorios árabes que controlan. Debido al malestar que provoca en este grupo terrorista, muchos gobiernos han recomendado su utilización como una forma de deslegitimación y contrapropaganda. Cabe señalar que, a lo largo de esta investigación, la denominación utilizada será indistintamente Dáesh o la forma abreviada “Estado Islámico”, cuya sigla es EI (IS, en su variante inglesa), y en tal caso le antecederá la palabra “autoproclamado” o “autodenominado”, en vista de evitar legitimar como un Estado a este grupo terrorista.

¹⁴⁶ BARRANCOS, David (2016): «Así recluta el EI: Ven a jugar al 'Call of Duty' de verdad/Entrevistado por Mayo Cerqueiro, Pablo», *Periódico El Español*, edición online de 15 de septiembre de 2016. Disponible en: https://www.elspanol.com/videojuegos/20151120/80741986_0.html [Fecha de consulta: 23 de junio de 2023].

simpatizantes, la radicalización de miembros terroristas y la incitación al terrorismo, pero es su narrativa y los usos tecnológicos aplicados lo que ha destacado al EI por sobre otros grupos terroristas.

El autoproclamado Estado Islámico ha desarrollado una narrativa transmedia caracterizada por el empleo de múltiples personajes y escenarios. Se trata de un estilo habitual en la industria audiovisual actual, propio de las series de *Netflix*, *Amazon Prime*, etc.¹⁴⁷, en donde se conjuga una historia breve sin un protagonismo único, con muchos personajes y con variados escenarios de acción. Este modelo de entretenimiento audiovisual aporta dinamismo a la historia y conecta principalmente con la audiencia más joven, acostumbrada en nuestro presente a la interacción múltiple que permiten los dispositivos electrónicos y las plataformas online. De acuerdo con Lesaca, “la fuerza del guión de estas historias reside en la interacción de personajes y escenarios” [...], y según el autor, “esa interacción es la verdadera protagonista de la trama”.¹⁴⁸ Previamente, exactamente en el año 2003, Henry Jenkins anticipó lo que sucedería años después en la industria audiovisual, al afirmar que, si bien un buen personaje puede sostener múltiples narrativas, un mundo interesante puede sostener múltiples personajes.¹⁴⁹ En términos de la e-yihad, este “mundo interesante” es el que presenta el Estado Islámico en Internet y al que adhieren a diario cientos de simpatizantes. Lesaca encuentra motivos de esta adhesión masiva en las técnicas actuales de narrativa audiovisual. Conforme al autor, Dáesh “aplicó al campo del terrorismo las técnicas más avanzadas de elaboración de guiones de las series de ficción y sagas de películas occidentales como *Juego de Tronos* o *Star Wars*”.

Cabe recordar que el principio comunicativo de la industria audiovisual del entretenimiento moderno en Occidente se caracteriza por centrar la atención en la interacción de los personajes (más que en los personajes en sí mismo), por el gran uso de tecnología aplicada, y por la variedad de plataformas y/o formatos de acceso para el consumo de este entretenimiento, como apps, páginas webs, sitios interactivos, podcast, short videos, etc. La unión de estos tres elementos (interacción, tecnología y plataformas) nos presenta las historias transmedia a las que Jenkins hacía referencia de forma temprana. Once años más tarde, las historias transmedia fueron producidas y consumidas en todo el mundo, para finalmente acabar siendo adoptadas por el terrorismo yihadista como un modo de conectar con el público más joven.

Otro aspecto fundamental que caracteriza a la yihad online de Dáesh es el uso masivo de las redes sociales como Instagram, *TikTok*, *YouTube*, X (ex *Twitter*) o *Facebook*, entre otras. Si bien el uso de estas redes facilita la difusión del mensaje y promueve la e-yihad entre diferentes públicos, se debe señalar que, desde un punto de vista estrictamente comunicativo, el uso de redes sociales puede representar en primera instancia un elemento controvertido para la organización terrorista por el escaso control que representa para su mensaje. En la actualidad, el simpatizante de EI no solo actúa como usuario consumidor de contenido virtual sino también

¹⁴⁷ Empresas de entretenimiento cuyo servicio de *streaming* (transmisión) permite la visualización online de contenido audiovisual mediante el sostenimiento de una cuota de suscripción.

¹⁴⁸ LESACA, Javier (2017), opus cit., p. 71

¹⁴⁹ JENKINS, Henry (2023): «Transmedia Storytelling», *MIT Technology Review*, *Humans and Technology*. Disponible en: <https://www.technologyreview.com/2003/01/15/234540/transmedia-storytelling/> [Fecha de consulta: 23 de junio de 2023].

como un productor del mismo. Este nuevo modelo de usuario, denominado produsuario¹⁵⁰, se origina en la existencia de un rol híbrido de los consumidores de información en Internet, y en el caso de la e-yihad del autoproclamado Estado Islámico ayuda a generar una escritura colaborativa y la construcción social del significado de la yihad en Internet, aun a riesgo para la organización terrorista de que su mensaje se desvirtúe o escape ligeramente a su control.

Es apropiado recordar que en el capítulo anterior (Capítulo 2: Internet como el espacio idóneo para una nueva oportunidad criminal) se explicaba el hecho de que el surgimiento de Internet ha permitido que las organizaciones terroristas puedan controlar su mensaje durante todo el proceso comunicativo, sin depender de la difusión de los medios de comunicación tradicionales. En la actualidad, el uso de Internet supone que el mensaje esté sujeto a un control por parte de las organizaciones terroristas que se extiende desde la idea creativa hasta la difusión en la red. Tal ejercicio de control durante todo el proceso comunicativo ha sido muy característico de la gestión narrativa de Al Qaeda. Podemos encontrar un claro ejemplo de esto en los mensajes vertidos en foros abiertos promoviendo, días antes de que se perpetraran, los ataques a las Torres Gemelas. En este caso, el control total de la narrativa no radica en la difusión de dichos mensajes sino en el hecho de que estos mensajes fueron creados y vertidos a la red por medio de cuentas de usuario pertenecientes únicamente a miembros de la organización. Para Manuel Torres Soriano esta situación no deja de ser paradójica, dado que, “a pesar de lo mucho que se habla de las oportunidades que brinda al terrorismo el anonimato de Internet”¹⁵¹ tanto los grupos yihadistas como los miembros de la subcultura del hacking yihadista necesitan labrarse una reputación, y por lo tanto no esconder su actividad ni su autoría.

Al Qaeda y Dáesh han utilizado Internet para sus fines terroristas. Ambos han creado contenido propagandístico y se han encargado de su difusión online. Ambas organizaciones han instrumentado nuevas formas de reclutamiento en la red, de radicalización y de incitación al terrorismo. Y ambas han justificado en Internet sus acciones terroristas (ataques terroristas, financiación del terrorismo, promoción sistemática del terror, ejecuciones, secuestro, tortura, etc.) en una narrativa construida con fundamentos del salafismo yihadista.¹⁵²

¹⁵⁰ El concepto de *produsage* es un neologismo propio de la Web 2.0 y se enmarca en la idea de las wikis colaborativas en donde participantes activos en el proceso de construcción de conocimiento se convierten en editores y productores de conocimiento, y no simplemente en consumidores de información.

¹⁵¹ TORRES SORIANO, Manuel (2016): «Tendencias en procesos de radicalización», en: *Cuadernos del Centro Memorial de las víctimas del terrorismo. Terrorismo internacional: análisis de la radicalización y estrategias de prevención*, N.º 2, diciembre 2016, (95-110), p. 105.

¹⁵² A priori es determinante reconocer la diferencia que existe entre el islam (visión religiosa) y el islamismo (visión política-religiosa). A partir de esta primera diferencia parten diversas ramas cuyas denominaciones en muchos casos han sido mal interpretadas o empleadas por parte de gobiernos, instituciones y medios de comunicación occidentales. A fin de no perpetuar este equivoco es relevante detenernos en el esclarecimiento de este punto antes de continuar avanzando.

Dentro del islamismo, entre otras ramas, encontramos el salafismo. El salafismo (o fundamentalismo islámico) es una corriente ideológica ortodoxa que postula el regreso a las fuentes o tradiciones originarias. El salafismo ha estado presente desde los inicios del islam hasta nuestros días y “durante todo este tiempo, surgieron cuatro tendencias, que constituyen las principales corrientes salafistas de la historia musulmana: el salafismo purista, el salafismo wahhabí, el salafismo moderno y el salafismo yihadista.” Véase: MONTANER PERALTA, Gonzalo (2020): *Están con nosotros o con los terroristas*. Santiago: Ariadna Ediciones, p. 89. Habitualmente “los medios de comunicación occidentales, [...], identifican al terrorismo islamista con el salafismo o fundamentalismo, sin embargo, la mayoría de los salafistas no aceptan el uso de la fuerza para el establecimiento de una sociedad islámica y, menos aún, la utilización del terrorismo como un medio admisible en su lucha”. Véase: *Ibidem*, p. 80.

No obstante, aun cuando no todos los salafistas son yihadistas, sí que es cierto que todos los yihadistas antes de convertirse al yihadismo, se reconocían a sí mismos como salafistas. Por consiguiente, podemos afirmar que una parte de los miembros que adhieren

Pero mientras que Al Qaeda realizaba todas estas acciones comunicativas online de forma unidireccional (desde Al Qaeda hacia el usuario de Internet) atendiendo a las directrices de una estructura interna piramidal y con una gestión comunicativa centralizada exclusivamente en los miembros de su organización; el autoproclamado Estado Islámico desarrolló una comunicación bidireccional (desde EI hacia el usuario de Internet, y viceversa) que estableció un dialogo entre EI y el usuario, y facilitó la creación de una extensa estructura horizontal e internacional, con una gestión comunicativa descentralizada pero basada sobre ejes temáticos predeterminados que facilitan una línea discursiva. De esta forma EI ha implementado una gestión comunicativa que extiende una invitación a cualquier usuario de Internet a interactuar, a crear y a difundir contenido sobre el yihadismo global.

En términos generales, atendiendo a la visión teórica de Castells, el modelo comunicativo del Estado Islámico en la red, en el que hay un amplio predominio del uso de redes sociales, “se trata de un escenario donde la naturaleza descentralizada de la comunicación manda, donde la simetría, la reciprocidad y las competencias igualitarias en tanto para enviar y recibir comunicación son protagonistas.”¹⁵³ Se podría decir entonces que, con relación a un usuario anónimo de Internet, Al Qaeda realiza lo que se conoce como transmisión de información, y que Daesh implementa un auténtico dialogo basado en la reciprocidad comunicativa. Este dialogo, característico del Estado Islámico, resulta a todas luces una visión novedosa y acertada sobre la propaganda terrorista en Internet, porque no solo se facilita propaganda yihadista al público, sino que se comunica con la intención de crear una relación empática con dicho público a fin de hacerlos sentir parte de la organización, y de esta manera acrecentar todo el tiempo el número de adeptos.¹⁵⁴

A tenor de esto, David Barrancos indica que “mientras que Al Qaeda quería tener el control absoluto sobre la comunicación [...] el Estado Islámico se dio cuenta de que era mucho más efectivo, sobre todo con herramientas como Twitter, poder descentralizar esa comunicación y distribuirla en todo el mundo”. Para Barrancos ello significa que “por una parte han perdido el control absoluto del mensaje, pero por otra, lo han convertido en una hidra a la que no le importa cuántas cabezas se corten” [...] “siempre van a seguir apareciendo más”.¹⁵⁵

Estos mensajes online nacidos en la retroalimentación con EI desarrollan una red comunicativa en Internet que se focaliza principalmente en la propaganda yihadista, y su fomento continuo

activamente al salafismo se convierten posteriormente al yihadismo y por ello “los salafistas que propugnan el uso de la fuerza como medio de acción suelen ser llamados yihadistas y corresponden a lo que la opinión pública suele identificar con el erróneo concepto de fundamentalismo islámico.” Véase: BOTTA, Paulo (2007): *El concepto de “Fundamentalismo Islámico”*. Buenos Aires: Centro de Estudios del Medio Oriente Contemporáneo (Cemoc); p.4

“La ideología salafista yihadista [yihadismo] tiene como idea central la consolidación de un califato global mediante la guerra santa o yihad (en una de sus acepciones), que persigue el sometimiento del mundo a una forma de islamismo donde impere la sharia a través de métodos violentos, como el terrorismo. El salafismo yihadista entremezcla una posición de retornar a los ‘primeros días’ del profeta Mahoma, por una cuestión de pureza en el actuar, con la misión de convertir a los ‘infieles’ [cristianos] al islamismo, incluso, como se mencionó, por la fuerza para concretar el califato.” Véase: MONTANER PERALTA, Gonzalo (2020), opus cit., p. 82.

¹⁵³ CASTELLS, Manuel (2009): *Comunicación y poder*. Madrid: Alianza Editorial.

¹⁵⁴ Según Barrancos, “un informe interno del Departamento de Estado de Estados Unidos publicado por el New York Times este verano [2016] sugiere que el EI está ganando la batalla en las redes sociales. El think tank estadounidense Brookings Institution estima que entre septiembre y diciembre del año pasado por lo menos 46.000 cuentas de Twitter estaban en manos de simpatizantes del grupo terrorista, con una media de 1.000 seguidores por usuario. El departamento de comunicación central está en Raqa, la autoproclamada capital del grupo yihadista, pero a su vez, los diferentes territorios bajo el control del EI tienen sus propios departamentos de comunicación.” Véase: BARRANCOS, David (2016), opus cit. Disponible en: https://www.elespanol.com/videojuegos/20151120/80741986_0.html [Fecha de consulta: 23 de junio de 2023].

¹⁵⁵ *Ibidem*.

por parte de simpatizantes de todas parte del globo sostiene una narrativa yihadista que acrecienta la banalización del mal y la propagación del odio.

Si bien es la más comentada, la propaganda de EI no solo se centra en promover el reclutamiento, la radicalización y la incitación al terrorismo, sino que también existe un discurso propagandístico orientado a legitimar su pretensión de convertirse en un futuro actor estatal del Sistema internacional. No debe obviarse el hecho de que la autodenominación de este grupo terrorista (Estado Islámico) es a todas luces una declaración de intenciones en sí misma, y que la finalidad de la violencia política de Dáesh tiene como objetivo, entre otros, la creación de un Estado propio entre Siria e Irak. El prefijo “Estado” revela entonces la pretensión de este grupo yihadista en dejar de ser percibido como una amenaza para pasar a ser reconocido como un Estado dentro del Sistema internacional. Lesaca advierte al respecto de este tema que la estrategia de comunicación del EI se erige sobre “la base de una narrativa transmedia atractiva y distribuida directamente a las audiencias potenciales para fortalecer las adhesiones...” [y que] “la calidad y cantidad de estas adhesiones pueden incluso convertirse en una amenaza que compita de manera directa con la legitimidad de un Estado-nación”.¹⁵⁶

Reconocer a Dáesh como un Estado implicaría no solo una fractura en el orden del Sistema internacional, debido a la naturaleza criminal de sus acciones terroristas ejercidas en y contra el propio Sistema internacional y contra la población de las regiones que controla, sino que también significaría una degradación del Derecho internacional y de las instituciones internacionales.

Aun en este panorama, Dáesh sostiene invariablemente la pretensión de ser legitimado como un Estado, y esgrime para ello argumentos que alimentan su narrativa en Internet orientada a esta finalidad. Para estos argumentos, además de las redes sociales, el Estado Islámico emplea otras vías de difusión online como son las revistas oficiales de la organización *Dabiq* (publicada entre 2014 y 2016) y *Rumiyah* (publicada entre 2016 y 2017).

Cabe señalar que, con independencia de las pretensiones de Dáesh, los Estados se sustentan sobre la base de criterios que le son propios al Derecho internacional.

Si bien la definición de qué constituye un Estado en derecho internacional se ha visto influenciada durante años por importantes avances, prevalecen criterios comunes hasta la fecha. Estos son: una población permanente (implica el fomento de las aspiraciones compartidas), un territorio determinado (se estima que actualmente el autoproclamado Estado Islámico ejerce su control sobre 200.000 km² aproximadamente¹⁵⁷), un gobierno efectivo (no necesariamente democrático), capacidad de mantener relaciones internacionales con otros Estados (no están claras las intenciones de EI al respecto, no obstante los miembros de las Naciones Unidas han reiterado en diversas resoluciones¹⁵⁸ su apoyo de independencia y soberanía de Irak y Siria sobre

¹⁵⁶ LESACA, Javier (2017), opus cit., p. 31.

¹⁵⁷ “El Estado Islámico en menos de un año casi ha doblado sus áreas de control, según señala el grupo de expertos sobre Mali en su último informe de agosto al Consejo de Seguridad de la ONU. El grupo terrorista ahora controla todas los círculos rurales de la región de Ménaka (noreste), y también amplía zonas del círculo de Ansongo en la región de Gao (norte), desde donde presiona a otras zonas.” Véase: «Al Qaeda y Estado Islámico se hacen fuertes en Mali tras la salida de Francia y en plena retirada de la ONU», *Europa Press*. Disponible en: <https://www.europapress.es/internacional/noticia-qaeda-estado-islamico-hacen-fuertes-mali-salida-francia-plena-retirada-onu-20231001083252.html> [Fecha de consulta: 17 de diciembre de 2023].

¹⁵⁸ Resoluciones del Consejo de Seguridad S/RES/2170 de 15 de agosto de 2014 y S/RES/2178 de 24 de septiembre de 2014 y en la 7226ª sesión del Consejo de Seguridad, celebrada el 28 de julio de 2014.

los territorios conquistados), la independencia del Estado Islámico (implica la capacidad político-económica para autoabastecerse y no depender de fuentes externas), legitimidad (la legitimidad de un nuevo Estado viene dada por su reconocimiento internacional¹⁵⁹).

Resulta indiscutible el hecho de que en la actualidad el autoproclamado Estado Islámico no cumple los criterios que debería cumplir según el derecho internacional para ser considerado un sujeto de Derecho (Estado), no obstante, resulta indiscutible el hecho de que estamos frente a un actor no estatal (grupo terrorista internacional).¹⁶⁰

Es determinante detenerse por un momento en el último criterio que posee el Derecho internacional para obtener la consideración de Estado: el criterio de legitimidad. Este criterio es de especial relevancia para Daesh porque es precisamente en el cumplimiento del mismo donde podría cambiar su estatus de político a jurídico. Debido a ello, existe en Internet una ingente cantidad de propaganda tendiente a legitimar la organización.

Conforme al Derecho internacional el reconocimiento de un Estado posee únicamente un carácter declarativo y político y, en ningún supuesto, confiere a la entidad un carácter jurídico. Así, si un Estado es reconocido por unos países, y no es reconocido por otros, ello no le impediría establecer relaciones diplomáticas y legales con los Estados que sí le han reconocido. El reconocimiento puede ser el resultado de un acto explícito y formal (por ejemplo, mediante una declaración), pero también puede ser implícito o tácito (por ejemplo, mediante la firma de un tratado), pero cualquier caso siempre se trata de un acto unilateral. Aun cuando se trata de un acto unilateral, prevalece la costumbre internacional, y los parámetros establecidos por las Naciones Unidas en su Carta en cuanto a la inadmisibilidad del uso de la fuerza para la adquisición territorial. Según López Nalda y Boulat, “un cambio en esta situación podría producirse si Iraq y Siria se disolvieran oficialmente, como ocurriera en la antigua Yugoslavia, un supuesto en el que los demás países no parecen interesados.”¹⁶¹

La legitimidad parte conceptualmente de la antítesis de la soberanía, en cuanto mientras que la soberanía recae en el pueblo e inspira la regla de la mayoría; la legitimidad pertenece, o no, a quien representa el poder, o a los encargados de elaborar y aplicar las leyes. De esta relación nace el derecho a mandar y la obligación de obedecer. En la configuración actual del Sistema internacional los Estados que son parte de este Sistema se sustentan en alguno de estos cuatro principios de legitimidad: electivo, hereditario, aristo-monárquico, y democrático. “El principio

¹⁵⁹ De acuerdo con la resolución ‘El reconocimiento de nuevos Estados y de nuevos Gobiernos’ del Instituto del Derecho Internacional (IDI, 1936) consiste en “*el acto libre por el cual uno o varios Estados constatan la existencia sobre un territorio determinado de una sociedad humana, políticamente organizada, independiente de cualquier otro Estado existente, capaz de observar las prescripciones del derecho internacional*”.

¹⁶⁰ La teoría de las relaciones internacionales establece que “*la noción de sujeto de derecho tiene que ver con las capacidad de ser titular de derechos y obligaciones en un orden jurídico, interno o internacional, mientras que la noción de actor no estatal tiene relación con la capacidad de influencia, con el poder.*” Véase: FERNÁNDEZ LIESA, Carlos R. (2018): «Sujetos de Derecho y actores no estatales: cuestiones de Derecho internacional», *Anuario español de derecho internacional*, N.º 34, p. 94

En los últimos años se ha acrecentado en el Sistema internacional los denominados Actores no estatales violentos (ANEV) en las relaciones internacionales, como los grupos terroristas y las organizaciones criminales. Estos actores “*están en el plano de la ilegalidad, [debido a ello] no cabe sino utilizar técnicas de cooperación y persecución incrementando el papel de los convenios internacionales, las políticas internacionales y la cooperación en su persecución y erradicación.*” *Ibidem*, p. 90

¹⁶¹ LÓPEZ NALDA, María/BOULAT, Pierre (2015): «El Estado Islámico, ¿puede considerarse un Estado según el Derecho internacional?», *Legal Today*. Disponible en: <https://www.legaltoday.com/practica-juridica/derecho-internacional/derecho-union-europea/el-estado-islamico-puede-considerarse-un-estado-segun-el-derecho-internacional-2015-04-22/> [Fecha de consulta: 23 de junio de 2023].

aristo-monarquico ha sido siempre inseparable del hereditario. El principio democrático ha resultado incompatible con el hereditario del que a duras penas ha tolerado algún residuo. El principio electivo, fundamental para las democracias, fue utilizado también por las monarquías, las aristocracias y por ciertas instituciones autoritarias como la Iglesia católica.” [...]. “En suma, los principios de legitimidad son justificaciones del Poder, es decir, del derecho a mandar.”¹⁶² Desde una perspectiva teórica todo principio de legitimidad se fundamenta en instrumentos de la razón que se puedan utilizar como argumentos para establecer sistemas de poder eficaz. Según Ferrero, “incluso el más estrafalario de los principios de legitimidad presupone una cierta racionalidad.”¹⁶³ La atribución de poder debe ser admisible, al menos para una parte de la población, de los miembros de una organización, o de un sistema. Por tal motivo Dáesh desarrolla, además de la habitual narrativa orientada al reclutamiento y radicalización, una narrativa propagandística tendiente a exponer la ideología legitimadora de su existencia, y de sus razones para constituirse como Estado y ser reconocido como miembro del Sistema internacional.

En este contexto cabe preguntarse: ¿cómo la violencia terrorista promovida por el propio Estado Islámico en Internet ayuda a su legitimación dentro del Sistema internacional?

Para Meghnad Desai, al introducir en el islamismo (visión político-religiosa del islam) el uso de la violencia se genera dentro de este islamismo una visión radical (islamismo yihadista o yihadismo) que se nutre de la fundamentación teológica para implementar un yihadismo global por medio de Internet.¹⁶⁴ De esta manera el grupo Estado Islámico se transforma en un asunto de las relaciones internacionales. Es en este modelo de teo-terrorismo en donde los fundamentos del islam y las citas del Corán representan la argumentación racional que busca adquirir mayor protagonismo que los propios actos violentos. Es decir, el terrorismo es una llamada de atención dentro del Sistema internacional, pero es la fundamentación teológica la base racional necesaria que se enfoca en legitimar al Estado Islámico como un verdadero Estado-nación.

Rodríguez-Serrano ha analizado narrativas de fundamento teológico orientadas a sustentar ideologías violentas, y ha desarrollado un análisis comparativo entre el nazismo y el yihadismo del Estado Islámico.¹⁶⁵ Sus estudios comparados lo llevaron a analizar la trilogía antisemita del cine nazi¹⁶⁶ para sustentar que la ficción y la producción audiovisual puede ser utilizada para justificar ideológicamente el sostenimiento y la legitimación de un sistema o una nación. Según el autor, se encuentran muchos paralelismos entre el régimen nazi y el Estado Islámico. No obstante, entre los múltiples puntos de similitud expone una diferencia sustancial entre ambos en el hecho de que mientras que la violencia nazi estaba diseñada para permanecer oculta a la opinión pública, la violencia yihadista se estructura a partir de la publicidad¹⁶⁷ y busca generar

¹⁶² FERRERO, Guglielmo (1998): Poder. *Los genios invisibles de la ciudad*. Madrid: Tecnos; pp. 79-81.

¹⁶³ *Ibidem*; p. 83.

¹⁶⁴ DESAI, Meghnad (2007): *Rethinking Islamism*. Londres: I.B. Tauris, p. 23.

¹⁶⁵ RODRÍGUEZ-SERRANO, Aarón (2017): «Narrativa audiovisual, ontología y terrorismo: paradojas comunicativas en los videos del Estado Islámico», *Palabra Clave*, 20 (1), pp. 96-115.

¹⁶⁶ Se trata de una trilogía audiovisual propagandística, desarrollada aproximadamente entre 1939 y 1941 por la producción cinematográfica alemana del Ministerio de Propaganda (oficialmente, Reichsministerium für Volksaufklärung und Propaganda) de Hitler, en donde abundan los planteos antihebraicos. Consta de *El judío eterno* (*Der ewige Jude*, 1940), de Fritz Hippler, *Los Rothschild* (*Die Rothschilds Aktien auf Waterloo*, 1940-1941) y *El judío Suss* (*Jud Süß*, 1940), de Veit Harlan. Esta trilogía constituyó la base del *Mein Kampf* de Hitler.

¹⁶⁷ Nos referimos aquí, por ejemplo, a la transmisión en vivo de atentados terroristas (modalidad en la que Al Qaeda fue precursor) o la difusión de videos de las ejecuciones.

un efecto en la opinión pública, e incluso crearla allí donde no la hay. Es decir, la comunicación ideológica del nazismo se centraba en exponer sus argumentos antisemitas y en señalar el tratamiento institucional que debían de recibir los judíos por parte del Estado. Por su parte, el Estado Islámico va más allá y establece su comunicación estratégica precisamente en donde el nazismo determina su autocensura: es decir en la publicidad y la promoción del terror.

Si bien la utilización de miedo es inherente al terrorismo, que la comunicación ideológica y legitimadora de Dáesh esté articulada en torno al uso de la fuerza es lo que genera su publicidad viral en Internet y dentro del Sistema internacional.

Esta decisión posee para la organización yihadista una doble vertiente: por un lado, le dificulta ser reconocido y legitimado como un nuevo Estado, pero por el otro lo catapulta como un indiscutible actor internacional.

PARTE II: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET

CAPÍTULO 4: LA POLÍTICA CRIMINAL DE LA UE ANTE EL YIHADISMO ONLINE

DEFINIENDO EL CONCEPTO DE POLÍTICA CRIMINAL

En términos generales, podríamos partir de la idea de entender la Política Criminal (PC) como la capacidad de decidir legítimamente en sociedad sobre el delito.

Ello se traduce en términos prácticos como la facultad de decidir sobre tres cuestiones: sobre los instrumentos normativos con los que se puede hacer frente al delito, sobre las medidas institucionales de control, vigilancia y represión, y sobre las diversas formas y medios de prevención del delito y de las conductas desviadas relacionadas con este.

En síntesis, la Política Criminal establece cuáles son aquellas conductas que se consideran punibles dentro de una sociedad y pronuncia la respuesta, jurídica, institucional y preventiva hacia las mismas. En otras palabras, y dicho de forma excesivamente simplificada, podríamos afirmar que la Política Criminal es la reacción ante los actos estatuidos como delitos.

Para Sánchez-Ostiz, la Política Criminal¹⁶⁸ posee un carácter práxico derivado del hecho de que su objeto “no es algo tangible empíricamente medible, sino acciones, expresiones de libertad humana.”¹⁶⁹ De acuerdo con este enunciado, el autor afirma que esta Política Criminal se construye, se desarrolla y se establece a partir de las conductas, las acciones, pensamientos e ideas, (es decir, a través de diversas “expresiones de libertad humana”) de diferentes sectores sociales, y que debido a ello, la Política Criminal no es algo estanco cuyo establecimiento suceda una sola vez, pertenezca invariable o esté sujeto de forma exclusiva a la capacidad decisoria de una sola parte. En este sentido, debemos abrazar la idea de que la Política Criminal deviene de una serie de acciones que referencian a diversos grupos del ecosistema social. Por tanto, estas acciones y/o expresiones de libertad humana a las que se remite Sánchez-Ostiz hacen alusión a la postura general adoptada por una sociedad dada y en un momento dado, frente a los delitos.

Dentro de una sociedad, son determinantes para el establecimiento de la Política Criminal, las acciones de diversos actores. Podemos encontrar que toda sociedad está integrada por dos tipos de actores, los actores primarios y los actores secundarios. Entre ambos se establece una posición común o una posición encontrada, en caso de que surjan discrepancias, de la Política Criminal. En el segmento de los actores primarios, encontramos al aparato institucional del Estado que otorga forma y estructura a una sociedad desde un punto de vista político, judicial, policial y administrativo, y que está conformada por los múltiples órganos que poseen las competencias formales estatales y autonómicas. En el segmento de los actores secundarios, hallamos una faz ciudadana y plural integrada por diversos grupos poblacionales que

¹⁶⁸ La acepción de ‘política’ en el concepto de Política Criminal no debe de interpretarse erróneamente como actividades fundamentadas en una opinión o ideología partidista, sino como la idea del ejercicio Aristotélico del conocimiento.

¹⁶⁹ SÁNCHEZ-OSTIZ, Pablo (2012): *Fundamentos de Política Criminal. Un retorno a los principios*. Madrid: Marcial Pons.

representan los múltiples intereses de la sociedad y que a su vez ejercen o pretenden ejercer cierto grado de influencia sobre las decisiones de los actores primarios.¹⁷⁰

Las decisiones adoptadas legítimamente dentro de una sociedad por diversas instancias formales como la Legislatura, la Judicatura, las Administraciones Públicas, etc., son parte de la capacidad decisoria de los poderes públicos que pueden considerarse por antonomasia acciones de los actores primarios en la Política Criminal de cualquier Estado. Finalmente, son actores primarios los poderes públicos autonómicos de dicho Estado y las Organizaciones Internacionales (OOII) de las que dicho Estado es miembro.

Teniendo en cuenta que las Organizaciones Internacionales no son parte de un Estado y que no poseen competencias formales¹⁷¹ dentro de este, y teniendo en cuenta también que las recomendaciones de las OOII hacia sus miembros no poseen obligado cumplimiento y solo actúan como meras indicaciones u orientaciones hacia los Estados, cabe preguntarse: ¿Por qué se considera entonces a las OOII como a un actor primario de la Política Criminal, y no como un actor secundario? Parte de esta explicación se encontraría en el hecho de que durante los últimos veinte años se desarrolla en el Sistema internacional una tendencia hacia la unificación de criterios para luchar contra todos aquellos crímenes que tienen repercusiones internacionales. Esta tendencia, promovida en gran medida por las diferentes Organizaciones Internacionales existentes en el mundo, insta a que todos los Estados adopten unos estándares mínimos, de carácter común, que tienden a una persecución global de determinados delitos transnacionales considerados especialmente graves, como es el caso del terrorismo.

Cabe recordar que este análisis monográfico centra su estudio específicamente en la Política Criminal de la Unión Europea, y a su vez, que la UE es una Organización Internacional que ha alcanzado un grado de integración regional sin equivalente en el mundo. Esta integración supera las áreas habituales de otros bloques regionales, y debido a ello ha llegado a tener una taxativa capacidad de injerencia en el derecho interno de los Estados parte. De esta forma, en la actualidad, cada Estado Miembro de la UE delega parte de su autonomía jurídica en beneficio de un derecho comunitario. En materias específicas como el derecho fiscal se ha alcanzado prácticamente un derecho común, y por consiguiente podemos hablar en este ámbito de la existencia de un derecho fiscal europeo.

Por el contrario, por su propia naturaleza, en otras materias jurídicas no existe un derecho propio europeo y por ello se promueve que las legislaciones nacionales se aproximen.

En la actualidad, el Derecho penal continúa siendo competencia exclusiva de cada Estado, pero admite recomendaciones de la UE que son adoptadas de buen grado, e implementadas con matices o diferencias dentro de las legislaciones nacionales de cada país. En conclusión, en

¹⁷⁰ Son actores primarios los poderes públicos estatales y autonómicos. Es decir, el Poder Legislativo, el Poder Ejecutivo (Gobierno y Administración [Sistema penitenciario, Cuerpos y Fuerzas de Seguridad del Estado]), y el Poder Judicial (Ministerio Fiscal [Procuradurías en algunos países de Latinoamérica, y Judicatura], el Gobierno Provincial, la Administración Provincial, los Entes locales (Servicios sociales, Prevención comunitaria, Policía local, etc.), y las Organizaciones Internacionales.

Son actores secundarios los grupos de presión. Es decir, los medios de comunicación, partidos políticos, y otros grupos de presión (sindicatos, asociaciones de víctimas, asociaciones profesionales, cámaras empresariales, organizaciones ambientalistas, organizaciones veganas, organizaciones feministas, organizaciones LGTBI, organizaciones no gubernamentales de desarrollo [ONGD], el sector financiero, las empresas, las asociaciones de consumidores, los grupos religiosos, las asociaciones profesionales, etc.).

¹⁷¹ Es decir, no poseen esa capacidad de decidir legítimamente dentro de una sociedad, a la que hacíamos referencia al inicio de este capítulo.

Europa, los EEMM son receptivos a las recomendaciones de las instituciones¹⁷² de la Unión Europea. Para explicar este punto, en la Tabla 2 se grafican los diferentes grados de integración regional en el mundo, y se ilustra la capacidad escalar (y por ende la capacidad acumulada de la Unión Europea en diversas materias), a partir de la integración inicial del grado 1.

Tabla 2. Nivel de integración regional de la Unión Europea.

GRADO DE INTEGRACIÓN	TIPO	CARACTERÍSTICAS	EJEMPLOS
1	Área de Libre Comercio	Los Estados se comprometen a eliminar los aranceles entre ellos, pero mantienen los aranceles propios frente al resto del mundo	Acuerdos de Asociación UE-PECO, Acuerdo Centroamericano de Libre Comercio (CEFTA), zona de Libre Comercio del Báltico (BAFTA), y otros.
2	Unión Aduanera	Los Estados se comprometen a eliminar los aranceles entre ellos, y adoptan un arancel común frente al resto del mundo	Mercado Común del Sur (MERCOSUR), Mercado Común del Caribe (CARICOM), Comunidad Andina (CAN), Mercado Común Centroamericano (MCCA), La Unión Aduanera de África Austral (SACU), y otros.
3	Mercado Común	Los miembros eliminan los aranceles entre ellos, adoptan un arancel externo común y remueven las restricciones al movimiento de factores de producción entre los países miembros.	Comunidad Económica Europea (CEE)
4	Unión Económica	Los Estados coordinan y armonizan sus políticas económicas.	Unión Europea (UE), Unión Económica y Monetaria de África Occidental (UEMOA)
5	Unión Monetaria	Los Estados comparten una moneda y una política monetaria común. Establecimiento de Banco o Fondo monetario común.	Eurozona (UE), Zona CFA (Franc des Colonies Françaises d'Afrique).
6	Unión Política	Los Estados desarrollan una política exterior y de seguridad común. Agencias de seguridad común. Reconocimiento mutuo de sentencias judiciales. Coordinación policial y judicial. Parlamento común. Instituciones, leyes (en materias restringidas) y presupuesto común.	Unión Europea (UE)
7	Estado Unificado	Los Estados asumen un estatus y un funcionamiento equivalente al de una sola nación.	Sin registro de ejemplos hasta la fecha.

Fuente: Elaboración propia. 2022.

Si tenemos en cuenta los límites del Derecho internacional y la prevalencia del derecho interno en la Política Criminal de un Estado, cabría considerar a las Organizaciones Internacionales como un actor secundario. No obstante, conforme a todo lo previamente reseñado, debemos de considerar a las OOII como un actor primario de la Política Criminal debido a que los Estados

¹⁷² Parlamento Europeo y Consejo de Europa.

miembro de la UE tienden de manera constante hacia una armonización del Derecho penal en la región.¹⁷³

Debe de tenerse en cuenta también que uno de los motivos que a lo largo de los años ha acrecentado la integración regional de Europa, es el cumplimiento de los objetivos de seguridad nacional de los Estados parte. Debido a ello, la capacidad de la Unión Europea como Organización Internacional para el establecimiento de la Política Criminal de la región se ha expandido y se ha desarrollado con matices más propios de un actor primario, que de un actor secundario.

Los actores secundarios de la Política Criminal se caracterizan por su capacidad de influencia en la capacidad decisoria de los actores primarios. El segmento de estos actores se encuentra compuesto por grupos específicos de representación social, y actúan como grupos de presión, y en ocasiones muy concretas (dependiendo de su grado de influencia en la sociedad) también como un agente de opinión pública.

En la actualidad existen grupos de presión que son representativos de gran parte de los intereses que poseen las sociedades modernas. Los grupos de presión agrupan a personas con intereses similares, cuya defensa de sus intereses y grado de influencia los consolida en actores secundarios.

Un actor secundario extremadamente relevante que integra también el grupo de los enunciados previamente son los partidos políticos. Como actor secundario merece, al igual que los medios de comunicación, un inciso puntual derivado del hecho de su capacidad de influencia y representación grupal. Conforme a Oñate Rubalcaba, los partidos políticos se caracterizan por las relaciones de poder que tienen lugar dentro y fuera de sus estructuras y por las luchas electorales para alcanzar el mismo. Este poder les confiere la capacidad de funcionamiento como actor, debido al hecho de que tienden a actuar como mediador entre el Estado y la ciudadanía.¹⁷⁴

Los partidos políticos son, como actor secundario, un gran hacedor de la Política Criminal debido al hecho de que son capaces de aglutinar, representar y capitalizar los intereses de determinados grupos poblacionales. Es decir, detentan un gran poder de representación social. Su objeto consiste siempre en la adquisición de votos en las elecciones como vía a la obtención de cargos públicos, para así ejercer esta representación de manera formal.

Es precisamente en esta representación formal, derivada de unas libres elecciones dentro de un sistema democrático, en donde miembros de un partido político pueden pasar de ser un actor secundario a ser un actor primario con capacidad formal de decisión sobre la Política Criminal de un Estado y fijar la agenda política de la misma durante su legislatura.

Finalmente, en el grupo de los actores secundarios no puede dejar de mencionarse de manera especial a los medios de comunicación. Los medios son el principal actor secundario debido a su enorme capacidad para crear opinión pública en relación con diversos temas que atañen a la Política Criminal de un Estado. Este grado de influencia hace que se lo identifique en la sociedad

¹⁷³ Cabe señalar que esta armonización no es taxativa, y no promueve la imposición de un ordenamiento jurídico común, por lo tanto, hay margen de actuación para los Estados.

¹⁷⁴ OÑATE RUBALCABA, Pablo (2005): «Participación política, partidos y nuevos movimientos sociales», *Revista mexicana de ciencias políticas y sociales*, N.º 194, pp. 103-136.

como el cuarto poder¹⁷⁵, y que los actores primarios lo tengan muy en cuenta a la hora de desarrollar la agenda pública.

Además, los medios de comunicación, en el desempeño habitual de sus acciones, muy a menudo actúan como interlocutor de diversos sectores sociales. De esta forma, por ejemplo, realizan una entrevista en profundidad a un analista experto en seguridad ciudadana, o emiten en directo el testimonio de una víctima de un delito, o brindan espacio a la denuncia pública del presidente de una asociación de vecinos para la vigilancia ciudadana, o transcriben párrafos literales de la declaración de la defensa o la parte acusatoria en un caso judicial penal. Todas estas acciones informativas no solo inciden en el desarrollo de la Política Criminal de un país, sino que también otorgan visibilidad a todo tipo de actores secundarios con una capacidad de influencia menor.

Por otra parte, los medios de comunicación darán mayor o menor visibilidad a estos otros actores secundarios según sus propios intereses ideológicos. De esta forma, por ejemplo, si estamos frente a un medio de comunicación más conservador éste preferirá entrevistar a un analista que adhiera a la tesis de aumentar el control social como método preventivo, o a un legislador que promueva una propuesta de ley que explique la necesidad del incremento de las penas privativas de libertad, o al familiar de la víctima de un crimen reclamando justicia. En este caso, por ejemplo, el medio buscará crear una opinión pública tendiente a una mayor punición para el control y la represión del delito, y enfatizar en los beneficios de una mayor seguridad en la sociedad.

Por el contrario, un medio de comunicación más liberal preferirá, entre otras opciones, realizar una entrevista a un abogado que profundice en la vulneración de derechos que supone la vigilancia ciudadana en Internet, o invitar al presidente de una Organización no Gubernamental de Desarrollo (ONGD) que evidencie estadísticamente la estigmatización social que existe sobre la población inmigrante en cuanto a la autoría de los delitos, o informar acerca de las malas condiciones de los centros penitenciarios. En este caso, la cobertura periodística tendería a enfatizar en la protección de los derechos humanos y en el establecimiento de una sociedad orientada más a la prevención del crimen y no tanto a su punición.

Cuanto más conservador o liberal sea el medio de comunicación, más orientadas hacia los extremos serán las posturas adoptadas en las coberturas informativas. Naturalmente esto nos lleva a considerar que existe una orientación ideológica del medio. Esta orientación ideológica responde al hecho de que no debemos de olvidar que los medios de comunicación son empresas y que como tales buscan, aun en el desempeño de sus funciones informativas, el cumplimiento de sus propios fines.

Conservador o liberal. En ambos casos el medio busca inferir en la opinión pública y a través de esta buscará influir en la capacidad decisoria de los actores primarios cercanos a su ideario político. Para ello, todo medio de comunicación se vale de dos herramientas: la *agenda setting*

¹⁷⁵ El concepto de ‘cuarto poder’ surge en paralelo al surgimiento del Estado moderno. El paso del sistema feudal al burgués que comenzó a constituirse con las revoluciones burguesas de los S. XVII y XVIII y de la independencia de Estados Unidos de América en 1776, supuso el establecimiento de un nuevo orden de poder. Aparece entonces la división de poderes (Poder Ejecutivo, Poder Legislativo y Poder Judicial) como un nuevo ordenamiento institucional, caracterizado por el equilibrio de un sistema en donde el poder controla al poder y cada uno de estos actúa como contrapeso de los otros dos. En paralelo, el surgimiento de la imprenta tiene lugar también en este periodo y se incrementa en las poblaciones la necesidad de contar con información acerca de las revoluciones de la época. De esta forma se gesta una incipiente participación ciudadana en los asuntos públicos. Esto, la aparición del sufragio universal y las continuas publicaciones de la época propiciaron que la prensa adquiriese una importancia enorme derivada de su gravitación política. Con todo ello, y la posterior modernización de los medios, nació lo que se conoce como ‘cuarto poder’ caracterizado por su influencia en la sociedad, por su capacidad de control sobre los tres poderes formales, y por su capacidad de crear opinión pública. Véase: DE LA VEGA, Julio Cesar (1988). *Diccionario consultor político* [verde]. Buenos Aires: Librograf editora; pp. 69-71.

y el *framing*. La *agenda setting* o la Teoría del Establecimiento de la Agenda establece qué asuntos son de relevancia informativa y qué importancia, espacio o cobertura deben de tener. Según McCombs y Shaw¹⁷⁶, la acción de los medios de comunicación determina que el público sea consciente o ignore, preste atención o descuide, priorice o relegue, determinados temas u acontecimientos. Que un medio de comunicación le de menor o mayor cobertura a un tema, o directamente decida ignorar un tema u acontecimiento y no darle cobertura en absoluto es la forma en que los medios intentan influir en los espectadores.

La *agenda setting* es una herramienta que permite la creación de opinión pública y es utilizada por los medios de comunicación a fin de decidir a priori cuáles son las noticias que transmitirán. Así, cada medio decide y fija la cobertura de temas que considera relevantes mientras que omite deliberadamente temas que considera prescindibles. Esta jerarquía de noticias, en ocasiones la establece el propio medio de comunicación, y en otros casos viene establecida de forma exógena por el grupo empresarial o conglomerado de medios al que un medio de comunicación pertenece. En cualquier caso, la *agenda setting* responde a los intereses del medio o los intereses comunes de diversos grupos informativos o grupos de poder con los que el medio se relaciona.

Cabe señalar que el establecimiento de la *agenda setting* por parte del medio, no significa la creación y/o difusión de noticias falsas, sino la priorización de contenidos reales. Es decir, el medio busca influir en el público creando una agenda pública de noticias existentes. Da a conocer algunas noticias y no da conocer otras noticias. Y, puntualmente en el primer caso, escoge cuánto tiempo y difusión le otorgará a cada hecho noticioso. De ahí que, en la aplicación de la *agenda setting*, el medio de comunicación no dice qué pensar, sino sobre qué pensar.¹⁷⁷ Como consecuencia de esto, las personas suelen incluir o excluir en sus conversaciones e intereses habituales la información que los medios incluyen o excluyen de su propia agenda informativa. Es decir, el público tiende a asignarle a ciertos temas la misma importancia asignada por los medios.

De esta forma el medio de comunicación se asegura sobre qué se debe crear un debate público y así ejerce su influencia en la sociedad. Tal influencia posee naturalmente efectos en una variedad de ámbitos sociales, y entre ellos, en la Política Criminal de un Estado.

Muy estrechamente relacionada se encuentra la Teoría del Encuadre o *framing*. Esta teoría explica la utilización de otro recurso utilizado por los medios de comunicación para el establecimiento y orientación de su influencia. En este caso el recurso es utilizado para la construcción de la realidad. Para Sábada,¹⁷⁸ la *agenda setting* está relacionada con la transferencia y la accesibilidad mientras que el *framing* con la interpretación del mundo. Esta teoría se basa en un encuadre constructivista de la noticia. Cuando un medio de comunicación presenta una noticia no lo hace como un observador neutral o desde un punto de vista objetivo, sino desde una orientación ideológica. Es decir, desde la orientación ideología propia del medio. Eso hace que existan, en cada medio, esquemas básicos para la transmisión de la noticia, a fin de que se interprete la información bajo esa ideología predeterminada. El encuadre noticioso incide en la forma en que el público pensará sobre determinados asuntos. El

¹⁷⁶ MCCOMBS, Maxwell E. y SHAW, Donald (1972): «The Public Opinion Quarterly», *Oxford University Press*, Vol. 36, No. 2, pp. 176-187. Disponible en: <https://www.jstor.org/stable/2747787> [Fecha de consulta: 1 de julio de 2022].

¹⁷⁷ COHEN, Bernard Cecil (1963): *The Press and Foreign Policy*. Princeton: Princeton University Press.

¹⁷⁸ SÁDABA, Teresa. (2008): *Framing: El encuadre de las noticias. El binomio terrorismo-medios*, Buenos Aires: La Crujía.

framing es el tratamiento que se le brinda a la noticia, a fin de que el espectador reciba un determinado punto de vista o enfoque.

Robert Entman, entiende el *framing* como el “proceso de selección de unos pocos elementos de una realidad percibida ensamblándolos mediante una narrativa que los muestra de tal manera que se promueva una determinada interpretación particular.”¹⁷⁹

Teniendo en cuenta la definición de Entman, el *framing* es una herramienta sumamente útil para influenciar la Política Criminal debido a su poder sobre el público para reforzar creencias sobre las causas de los conflictos, atribuir responsabilidades sobre el tratamiento del delito, etc. Es decir, es un proceso que afecta al discurso de las noticias y, por ende, a la conceptualización y asimilación social de todas las cuestiones políticas.

Mediante el *framing* y la *agenda setting* los medios de comunicación buscan influir en las audiencias y crear un sesgo de pensamiento. Es por ello por lo que no podemos hablar de la Política Criminal sin antes remitirnos a sus actores y su grado de influencia y responsabilidad sobre el establecimiento de la misma.

La interacción entre los actores primarios y secundarios que deriva en el establecimiento de la Política Criminal de un Estado no solo tiene implicaciones en los aspectos prácticos de una sociedad tales como, por ejemplo, su política de Estado frente al terrorismo. Posee también pormenores normativos¹⁸⁰ en la población de la sociedad, estableciendo un modelo de conducta propio. Es la interacción que describe Habermas entre la formación institucional organizada y el espacio público, excepto que Habermas (incorrectamente a nuestro juicio) no observa en ese espacio público no organizado formalmente, la existencia de relaciones de poder.

«La expectativa normativa de resultados racionales se funda en la interacción entre la formación institucional organizada de la voluntad política y las corrientes de comunicación espontáneas de un espacio público no distorsionado por relaciones de poder, de un espacio público no programado para la toma de decisiones y en este sentido “no organizado”. “Espacio público” opera en este contexto como un concepto normativo. Las asociaciones libres constituyen los nudos de una red de comunicación que surge del entretnejimiento de espacios públicos autónomos. Tales asociaciones están especializadas en la generación y difusión de convicciones prácticas, es decir, en descubrir temas que sean relevantes para la sociedad global, en hacer contribuciones a las posibles soluciones de problemas, en interpretar valores, en producir buenas razones, en devaluar otras. Sólo pueden resultar eficaces de forma indirecta, es decir, introduciendo desplazamientos en los parámetros de formación organizada de la opinión y la voluntad a través de un cambio de actitudes y valores que pueda acabar afectando a mayorías.»¹⁸¹

Conforme a todas las enunciaciones previas queda manifiesto que la capacidad para desarrollar la Política Criminal de un Estado la detentan en conjunto dos tipos de sujetos, los descriptos como los actores primarios y los descriptos como actores secundarios. De ello deriva el entendimiento de que la Política Criminal no es algo que se establezca a decisión de una sola parte o instancia de la sociedad, sino que es una construcción conjunta entre diversos sujetos que son parte de la estructura formal o ciudadana de un Estado, y en donde cada actor realiza su aportación. No obstante, ello no debe dar lugar a una interpretación de la Política Criminal como

¹⁷⁹ ENTMAN, Robert M. (2007): «Framing Bias: Media in the Distribution of Power», *Journal of Communication*, 57, (163-173), p. 163.

¹⁸⁰ Ref.: normas sociales, no jurídicas.

¹⁸¹ HABERMAS, Jürgen (1998): *Facticidad y validez*, Madrid: Trotta; p. 611.

el resultado de la sumatoria de las acciones individuales de cada sujeto¹⁸², sino que debe ser entendida como el resultado de la interacción del conjunto de todos los actores. En ese sentido, las expresiones de libertad humana a las que nos referíamos al principio no crean la Política Criminal a voluntad de quien ostenta y/o ejerce esa libertad, sino que expresan una parte constitutiva de la voluntad del conjunto del Estado, integrada por los actores primarios y secundarios antes señalados.

La única diferencia subrayable entre los actores primarios y secundarios es aquella por la cual se identifica a los actores primarios con una mayor capacidad de poder ejecutivo, y a los actores secundarios con una mayor capacidad de influencia. Pero ambos ayudan a crear la Política Criminal de un Estado. En conjunto, los actores primarios poseen las competencias formales atribuidas por el ordenamiento jurídico, y por ello son quienes adoptan las leyes y determinan la agenda política, entre otras cuestiones, y los actores secundarios influyen sobre las decisiones y las medidas que los actores primarios utilizan o pretenden utilizar para combatir la criminalidad.

Ese ejercicio de libertad humana al que hacíamos referencia adquiere entonces matices diferentes según qué actor la practique. Lo reseñable es que únicamente en la práctica de este dialogo entre ambos actores es donde se expresa realmente cuál es la posición de un Estado frente al delito. Esta posición es el resultado racional de una interacción entre ambos actores, y de esta forma se otorga la legitimidad necesaria a la Política Criminal para que tenga impacto en la totalidad de la población. Ello se traduce en elementos tangibles como la posición que tiene dicho Estado frente a temas como el incremento o la reducción de las penas privativas de libertad, el sistema penitenciario, la reincidencia, la tipificación de los delitos en el Código Penal, la política migratoria de un país, el tratamiento de los delitos en los medios de comunicación, el régimen de menores, los derechos humanos, la opinión pública sobre los delitos, sistemas de denuncia, la profesionalización de los Fuerzas y Cuerpos de Seguridad del Estado, el presupuesto, los modelos de prevención del delito, las acciones de intervención comunitaria, la formación docente para la detección temprana del delito en los centros educativos, las diversas formas de control social, la vigilancia ciudadana, urbanismo y prevención ambiental, el uso de Internet, campañas de información preventiva, etc.

En conjunto podemos afirmar que todo Estado adopta una Política Criminal adecuada a la ideología que ostenta la Administración de un gobierno en funciones (actores primarios) y al conjunto de los sectores sociales (actores secundarios) que describíamos previamente. Naturalmente, esta Política Criminal puede variar y encontrar resistencia por parte de otros actores de la sociedad, o pueden existir propuestas inversas entre la visión del delito de los actores primarios y la visión del delito de los actores secundarios. No obstante, lo relevante es que será solo la ideología del conjunto la que determinará siempre la posición de un Estado frente al delito. Esta ideología es la que permitirá el establecimiento de un funcionalismo estructural a fin de que la sociedad alcance sus metas respecto a la Política Criminal que ha escogido para sí misma.

¹⁸² Este es el postulado tradicional de Charles Wright Mills quien entendía a la conciencia colectiva como la sumatoria de las conciencias individuales de los miembros de una sociedad. Por el contrario, el establecimiento de la Política Criminal adhiere más a la tesis *parsoniana*, de la realidad por la cual se produce una asimilación de los individuos hacia el entramado social, y de esta forma el orden social es percibido como un todo insoluble.

Podemos entender el funcionalismo estructural como el proceso por el cual se establece entre todas las partes la búsqueda de metas colectivas. Esto es especialmente relevante en el ámbito de la Unión Europea, en donde existe una organización política supranacional en la que, por obvias razones, existe una mayor pluralidad de actores primarios y secundarios.

No obstante, con independencia del objeto académico de este texto, es importante aproximarse a la idea de Talcott Parsons por la que se entiende que, “esa colectividad puede ser cualquier sistema que comprenda la acción coordinada de una pluralidad de individuos orientados hacia la consecución de una meta colectiva o de un sistema de metas colectivas. En este sentido, las colectividades abarcan desde grupos muy pequeños hasta el aspecto político de lo que Roscoe Pound denominara Sociedad Políticamente Organizada”, refiriéndose puntualmente a un Estado o a las comunidades intersocietarias como lo son los bloques regionales.¹⁸³

Una vez definida la importancia de los actores de la Política Criminal, estamos en posición de establecer algunas definiciones sobre este concepto. Una breve aproximación nos permite señalar que la Política Criminal es la adopción de estrategias que se orientan a la prevención, el control, la investigación y la sanción de la criminalidad, así como a la atención a las víctimas y el tratamiento de los condenados.

La Sentencia C-646 de 2001, emitida por la Corte Constitucional de Colombia recoge una amplia definición del concepto:

[La Política Criminal] es el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción. Dicho conjunto de respuestas puede ser de la más variada índole. Puede ser social, como cuando se promueve que los vecinos de un mismo barrio se hagan responsables de alertar a las autoridades acerca de la presencia de sucesos extraños que puedan estar asociados a la comisión de un delito [...]. También puede ser jurídica, como cuando se reforman las normas penales. Además, puede ser económica, como cuando se crean incentivos para estimular un determinado comportamiento o desincentivos para incrementarles los costos a quienes realicen conductas reprochables. Igualmente puede ser cultural, como cuando se adoptan campañas publicitarias por los medios masivos de comunicación para generar conciencia sobre las bondades o consecuencias nocivas de un determinado comportamiento que causa un grave perjuicio social. Adicionalmente pueden ser administrativas, como cuando se aumentan las medidas de seguridad carcelaria. Inclusive pueden ser tecnológicas, como cuando se decide emplear de manera sistemática un nuevo descubrimiento científico para obtener la prueba de un hecho constitutivo de una conducta típica.¹⁸⁴

Si bien esta se trata de una pronunciación bastante generalizada, nos sirve como punto de partida en nuestra conceptualización, dado que plantea la respuesta del Estado más allá de la opción jurídico-punitiva.

¹⁸³ FERNÁNDEZ CARDOSO, S. (2011). «Teoría, sociedad y poder en Talcott Parsons, C. Wright Mills, Jürgen Habermas y Anthony Giddens», Tesis de Doctorado, Universidad Católica Argentina, Facultad de Ciencias Sociales, Políticas y de la Comunicación, Buenos Aires: UCA, p. 101. Disponible en: <http://bibliotecadigital.uca.edu.ar/repositorio/tesis/teoria-sociedad-poder-talcott.pdf> [Fecha de consulta: 22 de junio de 2022].

¹⁸⁴ OBSERVATORIO DE POLÍTICA CRIMINAL (2015): *¿Qué es la política criminal?*, Dirección de Política Criminal y Penitenciaria, Ministerio de Justicia y del Derecho de Bogotá, Bogotá, D.C., DC-001/2015, pág. 4.

En términos generales, la Política Criminal ha sido casi siempre entendida como la política de seguridad. Según Baratta¹⁸⁵, Sozzo¹⁸⁶ y Pegoraro¹⁸⁷, persiste, con ello, una dicotomía en torno a la noción de seguridad-inseguridad que se resuelve habitualmente en términos de defensa del orden social. En esta tradición, la Política Criminal ha tendido a buscar el establecimiento de una lógica en donde impera la triada de orden social-Estado-política penal.

Sanz Mulas, en línea con este pensamiento, define la Política Criminal como el “conjunto de medidas (jurídicas, sociales, educativas, económicas, etc.) que adopta una sociedad políticamente organizada para prevenir y reaccionar frente al delito, a efectos de mantenerlo en unas cuotas tolerables”. Este conjunto de medidas y el establecimiento de cuotas tolerables del delito suelen estar en consonancia con la cosmovisión de la época. En consecuencia, respecto de las decisiones que una sociedad toma frente al delito, el delincuente, la pena, el proceso y la víctima es, *sensu stricto*, el cariz ideológico y su carácter esencialmente político el aspecto más relevante y definitorio de la Política Criminal de un Estado. Por ello, Sanz Mulas es determinante al expresar que “detrás de cada opción jurídica (constitucional-penal) hay una determinada opción política que se corresponde con la ideología hegemónica en ese momento.”¹⁸⁸

Esta visión de ideología hegemónica y sustentadora de la Política Criminal del momento es inherente a cualquier modelo de sociedad con independencia del sistema de gobierno que posea. Siempre que exista un sistema y Derecho penal estaremos frente a una ideología legitimadora que ha creado y pensado de forma previa a dicho sistema y derecho. Es decir, el modo de pensar la sociedad es anterior al establecimiento de cualquier Política Criminal.

No debemos asumir que una ideología hegemónica está vinculada necesariamente a la existencia de gobiernos antidemocráticos. Si bien tradicionalmente, en el imaginario cultural, pensar en términos de hegemonía nos remite a regímenes o modelos de actuación imperativos, la idea de ideología hegemónica del momento a la que se refiere Sanz Mulas describe el sistema de creencias de la época que actúa como antesala para el establecimiento de una Política Criminal determinada.

En las sociedades modernas, ese sistema de creencias es con estricto arreglo a valores democráticos y derechos fundamentales, y debido a ello no es admisible la visión de una Política Criminal dogmática y/o dictatorial tan propia de las tiranías.

En un Estado democrático, la ideología hegemónica se construye mediante un dialogo entre una pluralidad de voces y este dialogo no se ve interrumpido por el resultado de unas elecciones. Ello significa que aun cuando prevalezca por la acción del electorado una opción política triunfadora, la ideología hegemónica no debe de ser la que imponga esta opción política triunfadora, sino la que se edifica como una opción política conjunta.¹⁸⁹ Esta opción política es

¹⁸⁵ BARATTA, Alessandro (1997): «Política Criminal: Entre la política de seguridad y la política social», en: CARRANZA, Elías (Coord.), *Delito y Seguridad de los Habitantes*, México, D.F.: Siglo XXI, pp. 80-95.

¹⁸⁶ SOZZO, Máximo (2000): «¿Hacia la Superación de la Táctica de la Sospecha? Notas sobre Prevención del Delito e Institución Policial», en: *Centro de Estudios Legales y Sociales*, Buenos Aires: CELS, pp. 1-61.

¹⁸⁷ PEGORARO, Juan (2001): «Derecha criminológica, neoliberalismo y política penal», *Delito y Sociedad*, 15/16, pp. 141-160.

¹⁸⁸ SANZ MULAS, Nieves (2019): *Política Criminal*. Managua: INEJ.; p. 22.

¹⁸⁹ Según González Guarda, “otro tema controvertido es si las políticas públicas en materia criminal deberían responder al programa de determinados gobiernos o constituir políticas de Estado, para sustraerlas a la variabilidad temporal y las coyunturas electorales y económicas”. Véase: GONZÁLEZ GUARDA, Claudio (2017): «La Política Criminal aplicada (PCA): La deriva de la Política Criminal hacia la política pública», *Nuevo Foro Penal*, No. 88, enero-junio, Universidad EAFIT, p. 201.

a la que hace referencia Sanz Mulas, y la misma se construye mediante la coexistencia de los diversos actores primarios y secundarios que hacíamos referencia al inicio. En un Estado democrático la prioridad es siempre el ciudadano. El Estado tiene el deber de reducir la delincuencia y tiene que hacerlo teniendo en cuenta el interés general, que es la convivencia. El Estado democrático no puede partir de la premisa de erradicar el delito, sino la reducción de este. La reducción implica un equilibrio entre una convivencia factible y un respeto a los derechos ciudadanos. Esta última afirmación se sostiene en el hecho de que, para la teoría criminológica, el delito es consustancial a la sociedad: donde haya sociedad va a existir el delito. Huertas Díaz (2009) citando a Émile Durkheim sostiene que el delito es algo natural y hasta necesario en la sociedad.¹⁹⁰ Ello significa que en una sociedad democrática cambian y (con una buena gestión) se reducen los tipos de delitos. Es decir, el delito se transforma, pero no se elimina.

Naturalmente esto no será así en Estados en donde los derechos fundamentales han permanecido o permanecen aún en suspenso como consecuencia del establecimiento de un sistema de gobierno no democrático en donde la pluralidad de actores primarios y secundarios se ha visto restringida y/o anulada. En este caso estaríamos frente a una Política Criminal propia de un Estado totalitario que limita la libertad de sus ciudadanos. La ideología hegemónica en este caso estaría constituida mediante un poder ilimitado del Estado que tendería a la uniformidad del pensamiento y debido a ello la Política Criminal de dicho Estado, entre otras cosas, no gozaría de garantías constitucionales en el proceso penal. Como finalidad última de este Estado totalitario encontraríamos la pretensión de erradicar el delito porque desea garantizar su propia subsistencia. En un Estado con estas características se adoptan medidas tendientes mayoritariamente a la instauración del miedo como una medida de prevención general negativa e ilimitada.

Si realizamos una breve revisión histórica veremos que la evolución del Sistema internacional ha facilitado la introducción en cada nación de principios básicos que tienden a limitar el poder (*ius puniendi*) del Estado. Estos principios han establecido un desarrollo y ejercicio de la Política Criminal atendiendo a la dogmática jurídica. Esta visión dogmática se apoya en los Principios de la Política Criminal (principio de necesidad, principio de proporcionalidad y principio de adecuación de la intervención), en los Principios de Derecho sancionador (principio de legalidad, principio non bis in ídem) y en los Principios de Derecho penal (principio de intervención mínima, principio de responsabilidad subjetiva y personal, principio de irresponsabilidad penal de personas jurídicas).

Esta evolución ha facilitado una nueva forma de entender la Política Criminal, ya no como una ideología hegemónica estatal con una finalidad exclusivamente punitiva y sin restricciones, sino como un modelo de ciudadanía crítica que se agrupa conforme a la exigencia de sus intereses. El resultado de esto es la comprensión de la Política Criminal tal y como se explicaba al inicio de este capítulo. Es decir, una Política Criminal que no atiende a los intereses de una parte en particular, sino que se construye vivamente con la interacción de todos los actores.

¹⁹⁰ Manifiesta con esto el hecho de que no todo delito se produce en beneficio propio, y cita el caso de Gandhi cometiendo el delito de desobediencia civil. Tal sería el caso también de la comisión de delitos que generan cambios legislativos, a partir de la comisión recurrente en la búsqueda de nuevos valores sociales que se plasman en el Código Penal (por ej. el derecho de los animales). Véase: HUERTAS DÍAZ, Omar (2009): «Durkheim: la perspectiva funcionalista del delito en la criminología», *Revista Criminalidad Policía Nacional DIJIN*, Bogotá, D. C., vol. 51, núm. 2, dic, pp. 103-115.

Naturalmente, dentro de este esquema la participación ciudadana, los grupos de presión, así como medios de comunicación y partidos políticos, estarán más o menos limitados en su accionar en relación con el grado de madurez democrática alcanzado por la sociedad de la que hablemos.

En su desarrollo evolutivo, la Política Criminal se ha detenido ampliamente en el entendimiento del delito, el delincuente, la pena y el proceso y la prevención. Esta ha sido por siempre la visión teórica dominante hasta la incorporación de una nueva variable de análisis por mucho tiempo no prevista: la víctima. Según Alessandro Baratta, la incorporación de esta última variable supuso un nuevo entendimiento, más enriquecido, más completo e integracionista de la Política Criminal. Esto significa que, para reducir las infracciones delictivas, el entendimiento del control de la criminalidad debe extenderse también hacia un control de consecuencias a partir de la inclusión de una visión victimológica.¹⁹¹

Según este autor,

«El instrumental no penal de los medios utilizables para controlar las infracciones delictivas y sus consecuencias resulta teóricamente indeterminado. Por otra parte, en la práctica corriente de las políticas criminales se produce una selección del número de variables realmente examinadas en la construcción de modelos operativos de control. La riqueza y la variabilidad del instrumental dependen de la posición teórica adoptada.

En los niveles más bajos de la escala encontraremos los modelos de la criminología administrativa de impronta etiológica, aplicables solamente al control de la criminalidad. En niveles superiores encontramos los modelos de la criminología etiológica, que se extienden al control de las consecuencias. Los niveles se elevan con los modelos de la criminología crítica, en la medida en que ésta recoge el paradigma del ‘etiquetamiento’ o de la reacción social, lo mejora y lo torna adecuado a la aplicación práctica, mientras que al mismo tiempo la finalidad del control se extiende hacia las consecuencias.

Política Criminal no es solamente un concepto complejo; es también un concepto problemático. Si de los modelos prácticos más limitados de la criminología administrativa salimos hacia aquellos más amplios de la criminología crítica, la riqueza y la variabilidad del instrumental de un control que asume siempre más dimensiones se aproximan a su indeterminación teórica. En sus niveles más altos de elaboración la Política Criminal, en cuanto género, es como un universo mucho más complejo de la especie ‘política penal’.»¹⁹²

Es importante destacar que, en la actualidad, el grado de madurez en el desarrollo de la Política Criminal de un Estado, adhiere en gran medida a su madurez democrática alcanzada, a fin de promover una visión más integradora que no solo apele a limitar la práctica punitiva del Estado frente a los delitos, sino también a promover los modelos de prevención, los modelos sofisticados de control y los modelos de control de consecuencias. Naturalmente existe una correlación directa entre esta madurez político-democrática de un Estado, con su riqueza y variabilidad instrumental para la implementación efectiva de estos modelos señalados.

Conforme a todo lo detallado previamente podemos afirmar que existe un consenso de que en un Estado como el actual, social y democrático de derecho, la prevención del delito constituye el objetivo esencial de la Política Criminal, y que este objetivo estará siempre limitado por el respeto de los derechos fundamentales.

En nuestro presente no debe entenderse a la Política Criminal únicamente sobre la base de la limitación que ejercen estos Principios básicos al *ius puniendi* del Estado. Por el contrario,

¹⁹¹ BARATTA, Alessandro (1997): opus cit., p. 83.

¹⁹² *Ibidem*, p. 84 y ss.

debido al actual abordaje multidisciplinario de los fenómenos criminales y las nuevas formas de criminalidad que existen en nuestro mundo físico y virtual, comienza a imperar el hecho de considerar las tendencias futuras y el tratamiento de la criminalidad como un problema de política pública.

González Guarda se refiere a esta tendencia de la Política Criminal consistente en la pérdida de influencia del Derecho penal tradicional en detrimento de un diseño de una Política Criminal con perspectivas teóricas propias de las políticas públicas, en donde priman los conceptos de rendimiento, gestión y aplicabilidad.

La complejidad que han adquirido los fenómenos criminales y la amplia variedad de nuevos delitos, principalmente en Internet, sugiere nuevos enfoques en donde el abordaje del delito deba de ser “de forma multidisciplinaria, convirtiendo su tratamiento en un problema de política pública.”¹⁹³

En el panorama contemporáneo de la Política Criminal destaca la tendencia hacia la idea de rendimiento y gestión. Esta modernización de la Política Criminal atiende a la eficiencia operativa y al cumplimiento de la Agenda pública. Esto significa que en el espacio público (real y virtual) las decisiones comienzan a incorporar criterios técnicos, racionales y económicos junto a los políticos. Esto a su vez permite a posteriori un proceso autoevaluativo sobre el análisis de políticas cuyo objetivo es explicar o entender de forma científica la lógica de las decisiones tomadas en una Política Criminal determinada. La utilidad práctica de este análisis radica en el hecho de que ayuda a producir políticas más eficaces y eficientes (al aumentar la información en la toma de decisiones políticas y al confrontar las decisiones políticas con el impacto que producen en la realidad), disminuye el poder y el aislamiento de las burocracias y políticos (ello se debe al hecho de que las políticas públicas se crean con la participación de analistas y expertos, no solo con políticos y legisladores, y al introducir la cultura de la evaluación de resultados), mejora y moderniza los procesos de administración.

Según González Guarda, el devenir histórico de la Política Criminal nos ha llevado desde un paradigma disciplinar “típicamente *foucaultiano*, donde el encierro del sujeto constituye su máxima expresión”, a un paradigma del control¹⁹⁴ caracterizado por “nuevas formas de control, donde sería protagonista, entre otros rasgos, el manejo del riesgo penal (actuarial), la gerencialización operativa del sistema penal y el énfasis en la prevención del delito a través de la vigilancia de la vida social.”¹⁹⁵

Con relación a esta nueva Política Criminal, se expresa González Guarda citando a Díez Ripollés:

«La Política Criminal se inserta dentro del conjunto de las Políticas Públicas, singularmente en el marco de las políticas sociales, y en consecuencia no puede entenderse ignorando la interacción y apoyo

¹⁹³ GONZÁLEZ GUARDA, Claudio (2017), opus cit., p. 186.

¹⁹⁴ Para González Guarda este paradigma del control implica un control penal en apariencia “*suave, difícilmente contrastable e ilusoriamente racional*”. Es un tipo de paradigma que posee vocación hacia la aplicabilidad y que está relacionado con lo que se conoce como “*sociedad del rendimiento o del cansancio*.” [Ahí donde se erigía] “*la sociedad disciplinaria de Foucault, que consta de hospitales, psiquiátricos, cárceles, cuarteles y fábricas*”, [ahora tenemos] “*una sociedad de gimnasios, torres de oficina, bancos, centros comerciales, etc.*” Es decir, “*la sociedad del siglo XXI ya no es disciplinaria, sino una sociedad de rendimiento*.” Y sus habitantes ya no se llaman a estar sujetos a la obediencia, sino al rendimiento. La conducta normal o anormal ya no está estricta y únicamente determinada por las instituciones disciplinarias, sino primordialmente por el propio sujeto que, en su búsqueda obsesiva de rendimiento, resulta el máximo emprendedor de sí mismo.

¹⁹⁵ *Ibidem*.

recíprocos entre todas ellas. La Política Criminal, como cualquier otro tipo de política pública, aspira a ser un agente de transformación social, si bien confinada a un segmento limitado del comportamiento social.»¹⁹⁶

Todo este nuevo paradigma nos lleva a lo que se conoce como Política Criminal Aplicada (PCA). González Guarda entiende por PCA lo siguiente:

«Creación de un cúmulo de herramientas conceptuales y acciones concretas para su aplicación inmediata en el manejo o gestión del sistema penal. Las cuales se materializan desde la Política Pública o desde la práctica del sistema. Con participación preferente, pero no exclusiva, de la Política legislativa penal.»¹⁹⁷

La PCA engloba el conocimiento del fenómeno criminal actualizado, las aportaciones de las nuevas disciplinas científicas, la identificación de los nuevos sujetos y la Política Pública. La PCA se centra en el dominio de conocimientos prácticos derivados del planteamiento de escenarios criminológicos artificiales, que permiten el desarrollo de productos o modelos de alta aplicabilidad para las diferentes sociedades del mundo. La PCA introduce un conocimiento binaural dado que contempla el conocimiento teórico (anticipando problemas imaginarios) y pragmático (resolviendo o previniendo problemas reales) del crimen. Es decir, valida o descarta supuestos o modelos teóricos contrastando los mismos con la realidad criminal que posee una sociedad. De este enfoque surge la necesidad de crear “productos tangibles de control social que sean inmediatos, eficaces y evaluables”¹⁹⁸

En la actualidad, algunas tendencias en Política Criminal están vinculadas a la internacionalización que ha experimentado el delito, sobre todo a raíz del fenómeno de la globalización, y de su impacto en el ámbito del Derecho penal. Esta internacionalización derivada del binomio crimen internacional-respuesta jurídico penal armonizada ha generado una Política Criminal caracterizada por la influencia que dichos procesos transnacionales han tenido hacia el interior de los Estados nacionales. En todo el Sistema internacional destaca el tratamiento del terrorismo yihadista, el cual ha dejado de ser un problema meramente local o nacional y se ha convertido en uno de carácter transnacional, obligando a que las medidas político-criminales ahora se definan y diseñen considerando un escenario global. En el caso específico del terrorismo yihadista en Europa podemos ver de forma notoria esta tendencia de la Política Criminal al adoptar la región una Política Criminal propia en esta materia.

EL TERRORISMO YIHADISTA EN INTERNET ENTENDIDO COMO UN GRAVE PROBLEMA DE SEGURIDAD EUROPEO Y LA POLÍTICA COMÚN DE SEGURIDAD Y DEFENSA (PCSD) DE LA UE EN REFERENCIA A ESTE FENÓMENO

Durante muchos años se ha considerado que el terrorismo era un problema de carácter interno de algunos Estados, cuya existencia y pervivencia era inherente a las tensiones políticas que se suscitaban dentro de cada territorio nacional. Esta cosmovisión ha facilitado en buena parte no solo el crecimiento¹⁹⁹ de este fenómeno como forma de expresión política violenta, sino

¹⁹⁶ *Ibidem*, p. 195.

¹⁹⁷ *Ibidem*, p. 202.

¹⁹⁸ Se consideran aquí los planes anti-delincuencia, las estrategias preventivas o instrumentos de reacción penal.

¹⁹⁹ Por desinterés del Sistema internacional al no considerarlo un problema criminal de especial gravedad para el globo.

fundamentalmente un tratamiento jurídico e institucional dispar. La potestad legislativa de cada Estado, aunado al hecho del entendimiento conceptual que cada sociedad posee sobre el terrorismo²⁰⁰, ha creado múltiples escenarios de erradicación de esta amenaza que oscilan entre una mayor y una menor punición.

La adopción por parte de una facción del islam²⁰¹ de esta forma de demanda violenta ha supuesto la materialización de un nuevo peligro internacional. El mundo se puso en alerta a partir del 11S, porque por primera vez un atentado ostentaba todas las características del nuevo terrorismo internacional, en donde un grupo terrorista no solo pudo hacer sentir los efectos de sus demandas en otro territorio, sino que desarrolló una expansiva tensión política que, por desconocida, sacudió por completo el Sistema internacional.

Introducía de esta forma la idea de que se podía trasladar o llevar el conflicto hacia otras latitudes, neutrales o no, mediante atentados a su población, infraestructura y/o instituciones políticas.

Este terrorismo, denominado ‘foráneo’ por Luis De La Corte Ibáñez, se transformó rápidamente en un problema internacional por su espectacularidad y sus efectos desestabilizadores.²⁰²

Los diversos atentados terroristas de origen yihadista acometidos dentro de la Unión Europea aceleraron la adopción de múltiples medidas con el fin de frenar el avance del yihadismo. Estas medidas de carácter normativo, institucional y preventivo²⁰³, adoptadas en respuesta a esta nueva forma de terrorismo internacional, han ido desarrollando paulatinamente la Política Criminal de la Unión Europea en torno a este fenómeno.

En paralelo, los EEMM han cooperado entre sí en el *know how* derivado de la curva de aprendizaje que este desafío ha supuesto para cada Estado, y han ido compartiendo las medidas de contrterrorismo adoptadas en su ámbito nacional.

Cabe señalar que tanto las medidas de la UE como las adoptadas dentro de cada EEMM han ido evolucionado a lo largo del tiempo, en virtud de la modernización del yihadismo para su comisión delictiva.²⁰⁴

²⁰⁰ Remite a la idea del problema conceptual en torno a la dificultad que persiste aún en nuestro presente para arribar a una definición conjunta de ‘terrorismo’ dentro del Sistema internacional.

²⁰¹ Aquí nos referimos expresamente al yihadismo global. Es pertinente recordar que el actual yihadismo global se inició con los miembros de las corrientes más conservadoras del islamismo suní, denominados salafistas. El salafismo propone un seguimiento de la religión islámica desde una literalidad de las normas islámicas del Corán, la *Sunnah* (forma de vida y acciones del profeta Mahoma), el *Hadiz* (declaraciones, acciones y aprobaciones o permisos tácitos del profeta Mahoma), y *As-Salaf* (vivencias de las tres primeras generaciones de musulmanes). De acuerdo con el salafismo, tales criterios deben ser reguladores de la vida de todo musulmán. La interpretación radical de estos preceptos dio origen al yihadismo salafista (remite a las bases teológicas), y a lo que hoy conocemos como yihadismo global (remite a la internacionalización de sus acciones).

²⁰² De La Corte Ibáñez, citando a Reinales, interpreta que en este terrorismo foráneo existió una evolución que se inició en el terrorismo transnacional y se orientó hacia el terrorismo internacional. Según el autor, el terrorismo transnacional se entiende como aquel terrorismo que se ha promovido por actores cuyas actividades han trascendido las fronteras del país al que pertenecen por origen. Ello facilita el establecer células o estructuras clandestinas en los países de destino con tres objetivos concretos: 1) movilizar recursos materiales y humanos (activar la financiación, adquirir armamento, desarrollar reclutamiento, etc.); 2) establecer zonas de refugio o clandestinidad para los líderes en dichos países extranjeros; y, 3) ejecutar atentados en dichos países. Es relevante destacar que no todo terrorismo transnacional es internacional. Para poder referirnos concretamente a terrorismo internacional deben darse dos condiciones: 1) que la ideología del grupo terrorista tenga por objeto producir sus efectos políticos en el propio Sistema internacional, a fin influir y modificar la estructura de este; y, 2) que la extensión de sus actividades se desarrolle en más de un país a la vez. Véase: DE LA CORTE IBÁÑEZ, Luis (2012), opus cit., p. 28.

²⁰³ Por ‘institucional’ nos referimos a la cooperación institucional estructurada que realiza actualmente la UE en el ámbito judicial y policial. Se estudiará cada tipo de medida adoptada en profundidad en los capítulos siguientes.

²⁰⁴ Nos referimos aquí al *upgrade* que supuso para el yihadismo el surgimiento de Internet, no solo para la comisión de sus atentados sino para la realización de nuevos delitos derivados del uso frecuente de la red. Es fundamental recordar aquí la clasificación de la UNODC descrita en el CAPÍTULO 3: EL USO YIHADISTA DE INTERNET Y LA E-YIHAD DEL AUTOPROCLAMADO ESTADO ISLÁMICO.

Las medidas de contraterrorismo llevadas a cabo por la Unión Europea (UE), más concretamente en la esfera criminal referida al uso de Internet con fines yihadistas, emanan de la necesidad de coordinar esfuerzos en la lucha contra el terrorismo de etiología religiosa, debido principalmente al uso sostenido de las Tecnologías de la Información y Comunicación (TIC) por parte del yihadismo con fines de reclutamiento, adoctrinamiento y adiestramiento militar.

Inicialmente la Unión Europea centró los esfuerzos de la Política Criminal de la región, promoviendo el desarrollo de un frente común entre los gobiernos nacionales de sus EEMM a fin de adoptar políticas europeas contra el terrorismo, contra el terrorismo yihadista, y específicamente contra el terrorismo yihadista en Internet. En esta misma etapa de respuesta, la Unión desarrolló normativa europea que le permitiesen tener un marco regulatorio propio con el cual operar dentro de la región. Debido a ello, la Unión Europea y el Consejo de Europa desarrollaron una variedad de instrumentos legislativos para facilitar la persecución de este fenómeno criminal hacia dentro de las fronteras de la Unión, y a su vez la UE promovió la armonización de las legislaciones penales internas en esta materia, a fin de luchar de manera coordinada y común contra el yihadismo.

Habida cuenta de la necesidad de profundizar en la respuesta de la Unión a esta modalidad criminal, se implementaron medidas que facilitasen la coordinación y cooperación institucional dentro de la Unión. Cabe señalar que la articulación institucional representa un peldaño más en la Política Criminal de la UE en la lucha contra el terrorismo.

Las medidas adoptadas tempranamente de índole normativo fueron las que permitieron el sustrato jurídico necesario para el desarrollo de acciones de cooperación, mediante la creación de las agencias e instituciones necesarias para implementar un control efectivo en esta materia. Muestra de ello es que, ya en diciembre de 2003, la UE adoptó la *Estrategia Europea de Seguridad*, la cual se ocupa de la dimensión exterior²⁰⁵ de la seguridad de Europa. Siete años después, en un informe elaborado por la Secretaría General del Consejo titulado *Estrategia de Seguridad Interior de la Unión Europea*, se identifica por vez primera al terrorismo ya no como un problema singular de los Estados sino como una amenaza de impacto transfronterizo dentro de la Unión. Este documento ha resultado determinante a la hora de interpretar y abordar el fenómeno del yihadismo debido a que los diferentes EEMM de la Unión comprendieron de forma prematura la capacidad global de este tipo de terrorismo, y la mayor velocidad y alcance que promueve el uso de Internet a sus acciones criminales.

Esta comprensión ha posibilitado el desarrollo de estrategias específicas en materia de terrorismo yihadista como la elaboración de normativa europea que permita la persecución del fenómeno, la creación de diversas agencias policiales y judiciales europeas coordinadas en la neutralización anticipatoria de las acciones violentas que libra la yihad en Europa, y el desarrollo de campañas preventivas coordinadas para evitar la radicalización y el reclutamiento de nuevos simpatizantes dentro de la región.

²⁰⁵ La dimensión exterior de la Unión Europea está determinada por las fronteras exteriores del espacio Schengen. Implica estar alerta a las amenazas del yihadismo en otras partes del mundo, y anticiparse a la forma en que estas amenazas externas pueden llegar a vulnerar la seguridad del espacio comunitario.

La seguridad ha sido siempre uno de los pilares fundamentales de los que la Unión Europea se ha ido ocupando a lo largo de los últimos treinta años, y ello indudablemente ha orientado la Política Criminal de la región y de sus EEMM.

Para comprender adecuadamente cómo se ha ido gestando la Política Criminal de Europa, es necesario analizar la evolución de la UE en materia de seguridad y defensa comunitaria desde su creación hasta nuestros días.

En 1993, con la entrada en vigor del Tratado de Maastricht,²⁰⁶ tuvo lugar la creación de la Unión Europea y se activó con dicho acto la denominada *Política Exterior y de Seguridad Común (PESC)*. Es relevante recordar que desde el primer momento en que tuvo lugar su creación, la Unión Europea basó su fundamento organizacional en tres pilares: las Comunidades Europeas -primer pilar-, la Política Exterior y de Seguridad Común (PESC) -segundo pilar-, y el ámbito de Justicia y Asuntos de Interior (JAI) -tercer pilar-. Estos tres pilares han sostenido a lo largo del tiempo todo el desarrollo de la UE, y es precisamente en la PESC donde la UE ha depositado todas las acciones conjuntas orientadas al mantenimiento de la paz y a la resolución de conflictos (dentro y fuera de la Unión) en materia de seguridad.

En términos de Política Criminal, la PESC ha sido pensada para actuar dentro y fuera de la Unión en materia de seguridad. Por un lado, promueve el hecho de incrementar la defensa y anticiparse a las amenazas que puedan menoscabar la seguridad europea, y por el otro, se orienta a propiciar el entendimiento y la promoción de la paz internacional. La Política Exterior de la PESC se fundamenta principalmente en el uso de la diplomacia y en el respeto a las normas internacionales²⁰⁷. Además, promueve el comercio, la ayuda humanitaria y la cooperación con terceros países²⁰⁸.

Sí bien el análisis de la Política Exterior de la UE propia de la PESC no responde específicamente a nuestro objeto de estudio, sí que es coyuntural al mismo debido al hecho de que representa la expresión de la Política Criminal de la UE hacia afuera de los límites de la Unión por medio de una acción diplomática orientada a la gestión de crisis, la cooperación, y la pacificación internacional, estableciendo para ello alianzas con socios estratégicos que garantizan el éxito de los intereses de seguridad de la región.

Desde el establecimiento de la PESC, “la UE está tratando de erigirse en un actor internacional relevante para asumir mayores cotas de responsabilidad global”.²⁰⁹

En el año 1999 tiene lugar el establecimiento de la *Política Europea de Seguridad y Defensa (PESD)*.²¹⁰ En ese entonces, la PESD actúa como un instrumento auxiliar y se cimenta como la

²⁰⁶ El Tratado de Maastricht es, junto al Tratado de Funcionamiento de la Unión Europea, uno de los tratados fundacionales de la Unión Europea. Fue firmado el 7 de febrero de 1992, y entró en vigor el 1 de noviembre de 1993.

²⁰⁷ Lleva a cabo esta labor mediante el Servicio Europeo de Acción Exterior (SEAE) que se desempeña como el servicio diplomático de la UE. El SEAE se compone de una red de 140 delegaciones distribuidas en todo el mundo y oficinas de enlace del Parlamento Europeo en cada Estado Miembro. Por medio de estas delegaciones y oficinas se encarga de fomentar y proteger los intereses de la UE.

²⁰⁸ Nos referimos aquí a países que no pertenecen a la Unión Europea. Por lo tanto, son todos aquellos que se encuentran fuera de las fronteras externas de la Unión.

²⁰⁹ DE CASTRO RUANO, José Luis (2015): «La evolución de la Unión Europea como actor en materia de seguridad y defensa. En busca de un relanzamiento siempre pendiente», *Cuadernos Europeos de Deusto*, Universidad de Deusto, Número Especial 01, pp. 19-48.

²¹⁰ La PESD se inició con el nombramiento de Javier Solana como Alto Representante (AR) para la PESC y tuvo una duración de siete años.

vertiente operativa armada de la PESC. La finalidad de la PESD ha sido establecer la construcción de Europa en términos de seguridad y defensa por medio de operaciones conjuntas y establecer las bases tempranas para todo el desarrollo de la Política Criminal Europea.

En el año 2003, en el marco de la PESC, se establece la *Estrategia de Seguridad Europea (EES)*²¹¹ para dar respuesta a las amenazas externas a la Unión. Esta Estrategia significó un hito dado que por vez primera se establecían objetivos cuantificables y comunes para defender los intereses de la UE en materia de seguridad. La Estrategia de Seguridad Europea (EES) es un documento que posee un enfoque amplio y es sin lugar a duda aquel que aportó, con una anticipación de trece años, el fundamento doctrinal para el posterior establecimiento de la Política Común de Seguridad y Defensa (PCSD) cuyas orientaciones han sido y son determinantes en la Política Criminal actual de la Unión Europea.

La *Política Común de Seguridad y Defensa (PCSD, anteriormente Política Europea de Seguridad y Defensa, PESD)* se establece en el año 2016. No obstante, se describe por vez primera en el año 2007, concretamente en el Título V, Sección 2 del Tratado de Lisboa (acuerdo internacional que modifica los tratados que son base fundacional de la Unión Europea: el Tratado de la Unión Europea, TUE; y el Tratado de Funcionamiento de la Unión Europea, TFUE).²¹² Desde el Tratado de Lisboa hasta la fecha de su materialización en el año 2016, la PCSD ha evolucionado considerablemente tanto política como institucionalmente, y ha manifestado siempre sus intenciones comunitarias en materia de seguridad y defensa por medio de una multitud de estrategias y de documentos.

La importancia indiscutible de la PCSD es que con ella se establece una nueva institucionalización en materia de seguridad y defensa. Hasta la fecha, con la PESD, la UE había operado en estos ámbitos dando respuesta operativa en situaciones de urgencia decisoria, y muy a menudo con limitaciones jurídicas o políticas. La PCSD introduce un reordenamiento institucional que estructura el funcionamiento de la UE en materia de seguridad y defensa al amparo de la Comisión y por tanto de una legitimidad permanente.

Enrique Mora Benavente expresa en relación con ello que,

«El Tratado de Lisboa introduce cambios sustanciales tanto en la PESC como en la nueva Política Común de Seguridad y Defensa, la PCSD. El más relevante es sin duda la profunda reordenación institucional que supone unir en una sola persona tres competencias antes repartidas en sendas instancias. El Alto Representante dirigirá a partir de ahora la PESC y la PCSD y lo hará contando con los medios de la Comisión (institución de la que es Vicepresidente) y la oportunidad de influencia política en la toma de decisiones que le otorga su papel de Presidente del Consejo de Asuntos Exteriores. Por primera vez desde su fundación, la Unión está en disposición de definir y ejecutar una auténtica política exterior. [...] Más allá de un cambio institucional profundo, el Tratado de Lisboa introduce innovaciones importantes en materia PESD al tiempo que da naturaleza jurídica y legitimidad de derecho primario a prácticas que se han venido haciendo a los largo de estos últimos siete años fruto de la necesidad. Como se ha señalado antes, la PESC y sobre todo la PESD se han definido día a día, en contacto con la realidad más inmediata, a la que había que dar a veces soluciones y respuesta improvisadas. Lisboa da carta de naturaleza a algunas

²¹¹ La EES también es conocida en España como *Documento Solana* por referencia directa a Javier Solana, Alto Representante para la Política Exterior y Seguridad Común (PESC) en el citado año de establecimiento de la EES. Véase: CONSEJO DE LA UNIÓN EUROPEA (2003): *Estrategia Europea de Seguridad (EES,2003): Una Europa segura en un mundo mejor*, Bruselas.

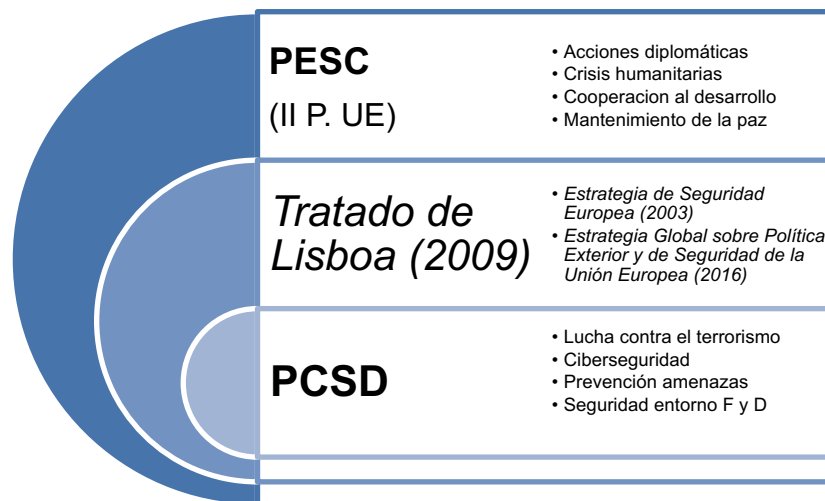
²¹² Antes de la introducción del Tratado de Lisboa, la Política Común de Seguridad y Defensa (PCSD) se denominaba Política Europea de Seguridad y Defensa (PESD), y contaba con orientaciones más reducidas.

de estas prácticas. Junto a ello, introduce dos compromisos jurídicos que traducen una elemental solidaridad de socios en la Unión: ante una agresión de un tercer Estado y ante un acto terrorista.»²¹³

La Política Común de Seguridad y Defensa (PCSD) se encuadra dentro de la PESC y, en su especificidad, responde a los intereses de seguridad y defensa de la Unión, y a la prevención de nuevas amenazas en la región. La PESC posee facultades más amplias y se encarga de la seguridad hacia dentro y hacia fuera de la Unión. Hacia dentro, la Política Criminal de la Unión Europea se materializa en la relación PCSD, y hacia fuera se proyecta hacia el Sistema internacional mediante la propia Política Exterior de la PESC.

Se puede observar de forma gráfica el origen de la PCSD dentro de la UE, y la forma en la que trabaja la PESC hacia afuera y hacia adentro de la Unión (en este último caso mediante la PCSD) en el gráfico a continuación:

Gráfico 4: Relación entre la PESC y la Política Común de Seguridad y Defensa (PCSD).



Fuente: Elaboración propia. 2023.

De Castro Ruano, explica detalladamente esta capacidad bicéfala de la PESC en el siguiente enunciado:

«La UE desarrolla una acción multifacética en el campo de la prevención de conflictos, mantenimiento de la paz, reforzamiento de la seguridad así como gestión civil y militar de crisis; la gestión de crisis internacionales se está convirtiendo en la dimensión más característica de la política exterior común. Este es un ámbito en el que confluyen tanto las relaciones exteriores de la Unión (acuerdos preferenciales y relaciones estructuradas de naturaleza político-económica con terceros; política de vecindad, cooperación al desarrollo, ayuda humanitaria, etc.; todas ellas concebidas como actuaciones que inciden en subsanar las causas estructurales de los conflictos) así como la PESC-PCSD y sus misiones operativas (que inciden en las crisis declaradas). Desde hace ya algunos años, la UE viene actuando en la gestión internacional de

²¹³ MORA BENAVENTE, Enrique (2010): «Introducción. La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa», *Cuadernos de Estrategia*, N.º 145, Marzo 2010, Instituto Español de Estudios Estratégicos. Ministerio de Defensa de España, pp. 19-20.

crisis, sea en respuesta a las demandas de la ONU o por el deseo de algunos Estados Miembros de ejercer un protagonismo político internacional en consonancia con su potencial económico. para ello se ha ido dotando de instrumentos de diferente naturaleza. a los instrumentos políticos y económicos con los que contó desde siempre, se añade posteriormente una capacidad autónoma de actuación en el ámbito de la seguridad y la defensa en el marco de la PESC y PCSD, y ahí va a residir su singularidad y valor añadido en materia de gestión internacional de crisis: su capacidad para movilizar una muy amplia gama de instrumentos de diferente naturaleza, tanto civiles como militares que le proporcionan, sobre el papel al menos, una capacidad global o «integral» de gestión de crisis. Es precisamente este «enfoque integral» (*Comprehensive approach*) que caracteriza la gestión internacional de crisis de la UE su rasgo más definitorio.»²¹⁴

En junio de 2016 se presentó ante el Consejo Europeo la *Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea*²¹⁵ (o Estrategia Global de la UE) para reforzar la defensa y hacer frente a los desafíos que presentaba el nuevo terrorismo. La Estrategia Global de la UE fue presentada por la VP/AR²¹⁶ Federica Mogherinise al amparo de la Agencia Europea de Defensa (EDA, European Defense Agency).²¹⁷ La Estrategia Global de la UE resulta un instrumento fundamental porque en él se define la estrategia para la PCSD. Es a partir de este momento en el que surgen diferentes vías propositivas de cooperación que rigen como el marco político que orientará la Política Criminal de la Unión Europea hasta nuestros días.

Por medio de la PCSD, los Estados Miembros desarrollarán una cultura estratégica de seguridad y defensa para proteger a la Unión y a sus ciudadanos. Esta cultura estará signada por una serie de estrategias y documentos orientados de forma permanente hacia la seguridad y defensa común, en los que el terrorismo internacional posee especial atención.

Así, en el año 2017 se establece la *Cooperación Estructurada Permanente (PESCO, Permanent Structured Cooperation)*²¹⁸ cuyo objetivo es profundizar la cooperación en materia de defensa militar cibernética. El objetivo principal de PESCO es mejorar la capacidad de la UE como actor de seguridad internacional, contribuir a la protección de los ciudadanos de la UE y maximizar la eficacia del gasto en defensa. En referencia a esta cooperación estructurada, HR/VP Josep Borrell ha pronunciado "Ampliaremos nuestra capacidad para hacer frente a las ciberamenazas, la desinformación y la interferencia extranjera".²¹⁹

²¹⁴ DE CASTRO RUANO, José Luis (2015), opus cit., pp. 23-24.

²¹⁵ Conocida sintéticamente como la Estrategia Global de la UE. Esta estrategia sustituye a la Estrategia de Seguridad Europea fundamentalmente por el hecho de que está última no responde adecuadamente a los actuales desafíos del entorno. Véase: COUNCIL OF THE EUROPEAN UNION (2016): A Global Strategy for the European Union's Foreign and Security Policy. 14392/16, Brussels, 14 November 2016.

²¹⁶ VP/AR: Vicepresidente de la Comisión/Alta Representante (*HR/VP: High Represent/Vice President*).

²¹⁷ La Agencia Europea de Defensa (EDA) impulsa a sus 27 Estados Miembros a la mejora de sus capacidades de defensa a través de la cooperación. Actúa como enlace con los Ministerios de Defensa dispuestos a participar en proyectos colaborativos. EDA se ha convertido actualmente en el epicentro de cooperación europea en materia de defensa. Actúa como una plataforma intergubernamental de expertos que investigan e implementan proyectos de colaboración. Los Estados Miembros pueden decidir uno a uno si participan en proyectos, en función de sus necesidades e intereses. La Agencia Europea de Defensa (EDA) ha sido creada el 12 de julio de 2004 mediante una acción común (2004/551/PESC) del Consejo de Ministros, y su base jurídica se encuentra descrita en el artículo 42.3 del Tratado de la Unión Europea (TUE). NOTA: No se utiliza aquí la sigla en español *AED* (*Agencia Europea de Defensa*) que la propia Unión Europea designa en su traducción al castellano, sino *EDA* (*European Defense Agency*) debido a dos motivos razonados: 1) La sigla en inglés *EDA* es una denominación comúnmente conocida y utilizada entre los EEMM y, 2) El Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, así como el Ministerio de Defensa de España, utilizan la denominación *EDA* para referirse a la Cooperación Estructurada Permanente desde que esta ha sido creada. Habiendo observado que estos dos motivos se reiteran en otros casos, se utilizará esta lógica de uso con las estrategias y políticas que se expliquen a posteriori. No obstante, en las Abreviaturas (ref.: índice de la tesis) se encontrarán listadas todas las denominaciones existentes.

²¹⁸ COUNCIL DECISION (2017): CFSP 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

²¹⁹ EU Strategic Compass for Security and Defence, HR/VP Josep Borrell, p. 6-7.

En ese mismo año tiene lugar la implementación de la *Revisión Anual Coordinada de la Defensa (CARD, Coordinated Annual Review on Defence)*²²⁰ se encuentra dentro de la Estrategia Global de la UE desarrollada por la Agencia Europea de Defensa (EDA, *European Defense Agency*). La CARD actúa como un proceso de seguimiento de los planes de defensa de los Estados Miembros de la Unión Europea para ayudar a coordinar el gasto e identificar posibles proyectos de colaboración. Su objetivo es brindar a los Estados Miembros un panorama de sus potencialidades en materia armamentística. Promueve también que los EEMM posean ciclos sincronizados de planificación en defensa nacional a fin de optimizar la capacidad defensiva europea.

En el año 2017 también se establece en el marco de la Agencia Europea de Defensa el *Fondo Europeo de Defensa (EDF, European Defense Fund)*²²¹ orientado a la investigación y desarrollo colaborativo en materia de defensa y el fomento a la industria defensiva. El EDF cofinancia proyectos de desarrollo colaborativo entre EEMM en materia de seguridad, investigación y desarrollo de prototipos para la defensa.

En el 2020 se establece la *Estrategia de la Unión de la Seguridad de la UE*²²² en sustitución de la Estrategia Global para la Política Exterior y de Seguridad de la UE del año 2016. La Estrategia de la Unión de la Seguridad de la UE abarca el periodo 2020-2025 por lo que aún se encuentra vigente. Los ámbitos prioritarios de este documento se orientan a la lucha contra el terrorismo, la delincuencia organizada, prevención y detección de amenazas híbridas y el incremento de la resiliencia de las infraestructuras críticas, la promoción de la ciberseguridad, y garantizar la seguridad del entorno físico y digital de Europa. El 16 de diciembre de 2020, en el marco de la Estrategia de la Unión de la Seguridad de la UE, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una nueva *Estrategia de Ciberseguridad de la UE*.²²³ Esta tiene como objetivo garantizar en Europa una Internet global, pero con salvaguardas contra riesgos a la seguridad y los derechos fundamentales. A su vez, en el marco de esta Estrategia de Ciberseguridad de la UE, se ha creado la Unidad Cibernética Conjunta²²⁴ que permite reforzar la cooperación entre las instituciones, agencias, organismos y autoridades de los Estados Miembros de la UE. Todo ello crea un gran ecosistema en materia cibernética orientado a la seguridad de Europa y hacia su soberanía defensiva, a fin de evitar ataques terroristas que amenacen su ciberseguridad.

Según el Centro Nacional de Inteligencia (CNI) español, el aumento de ataques a infraestructuras críticas ha ido en aumento desde el año 2018, sin embargo, específicamente los yihadistas no han perpetrado hasta la fecha del informe (año 2019) ningún ciberataque significativo.²²⁵ No obstante, debido al curso actual y la progresiva curva de aprendizaje que

²²⁰ Revisión Anual Coordinada de la Defensa (*CARD, Coordinated Annual Review on Defence*). Disponible en: [https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-\(card\)](https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)) [Fecha de consulta: 03 de noviembre de 2023].

²²¹ Agencia Europea de Defensa el Fondo Europeo de Defensa (EDF, *European Defense Fund*). Disponible en: [https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-\(edf\)](https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)) [Fecha de consulta: 03 de noviembre de 2023].

²²² COMISIÓN EUROPEA (2020): *Estrategia de la UE para una Unión de la Seguridad: integrar las medidas individuales en un nuevo ecosistema de seguridad*. Bruselas, 24 de julio de 2020.

²²³ JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Disponible en: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> [Fecha de consulta: 12 de noviembre de 2023].

²²⁴ Unidad Cibernética Conjunta, *Comisión Europea*. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/joint-cyber-unit> [Fecha de consulta: 12 de noviembre de 2023].

²²⁵ CENTRO CRIPTOLÓGICO NACIONAL. CNI (2019): IA-13/19. Ciberamenazas y tendencias 2019. CNN_CERT Resumen Ejecutivo, p. 7.

están teniendo los terroristas, se vaticina que solo es cuestión de tiempo para que el uso de Internet con fines yihadistas evolucione desde la propaganda hacia la ciberguerra.²²⁶ Debido a ello, tal como la propia Estrategia de Ciberseguridad de la UE indica:

«La soberanía tecnológica de la UE debe basarse en la resiliencia de todos los servicios y productos conectados. Las cuatro cibercomunidades (aquellas que se ocupan del mercado interior, de la aplicación de la ley, de la diplomacia y de la defensa) deben trabajar más estrechamente para lograr una conciencia compartida de las amenazas. Deberían estar preparados para responder colectivamente cuando se materialice un ataque, de modo que la UE pueda ser más que la suma de sus partes. La estrategia cubre la seguridad de servicios esenciales como hospitales, redes eléctricas, ferrocarriles y el número cada vez mayor de objetos conectados en nuestros hogares, oficinas y fábricas. La estrategia tiene como objetivo desarrollar capacidades colectivas para responder a los principales ciberataques. También describe planes para trabajar con socios de todo el mundo para garantizar la seguridad y la estabilidad internacionales en el ciberespacio. Además, describe cómo una Unidad Cibernética Conjunta puede garantizar la respuesta más eficaz a las amenazas cibernéticas utilizando los recursos colectivos y la experiencia disponible para los Estados Miembros y la UE.»²²⁷

En el curso de esta Política Criminal orientada a la protección europea, en el año 2021 se instaura el *Fondo Europeo de Apoyo a la Paz (EPF, European Peace Fund)*²²⁸ que faculta a la UE a colaborar con sus socios internacionales brindando insumos militares e infraestructura de seguridad.

Y finalmente, en 2022, se pone en marcha la *Brújula Estratégica para la Seguridad y la Defensa (Brújula Estratégica de la UE o Strategic Compass)*.²²⁹ Este instrumento facilita la evaluación del entorno en el que opera la UE con el objeto de detectar amenazas y desafíos actuales en el ámbito físico y digital. Tal y como el propio documento rector expresa "En el ámbito cibernético, nuestras fuerzas deben operar de manera coordinada, informada y eficiente".²³⁰ En cualquier caso, busca desarrollar la capacidad de seguridad de la UE basándose en cuatro pilares: actuar, invertir, asociarse y proteger. La Revisión Anual Coordinada de la Defensa (CARD), implementada en el año 2017, sirve como una herramienta importante para hacer avanzar la Brújula Estratégica de la UE.

La UE no posee un ejército propio, debido a ello debe recurrir a la asociación y coordinación de las fuerzas nacionales de cada uno de sus EEMM para responder a cualquier tipo de amenaza que requiera de intervención o despliegue conforme con los requerimientos específicos de la PCSD. Es por esto mismo que un elemento clave en la PCSD lo constituye el reforzamiento de las capacidades militares nacionales, lo cual no significa gastar más, sino gastar mejor y más coordinadamente a fin de optimizar la inversión de cada Estado Miembro.

Si bien la inversión promovida por la PCSD se orienta al fortalecimiento común de la Unión Europea como Organización Internacional, los efectos de dicha inversión generan un inevitable

²²⁶ Manuel Torres Soriano citando a Mike McConnell, ex Director de Inteligencia de los Estados Unidos, describe que "los grupos terroristas de hoy día se sitúan en la parte inferior de la capacidad de ciberguerra [...], pero tarde o temprano lograrán la ciber-s sofisticación. Es igual que la proliferación nuclear, solo que más fácil." Véase: TORRES SORIANO, Manuel (2015): «¿Es el yihadismo una ciber- amenaza?», *Revista de Occidente*, no 406, marzo 2015, p. 8-9.

²²⁷ Estrategia de Ciberseguridad. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-strategy> [Fecha de consulta: 12 de noviembre de 2023].

²²⁸ Fondo Europeo de Apoyo a la Paz. Disponible en: <https://www.consilium.europa.eu/es/policies/european-peace-facility/> [Fecha de consulta: 03 de noviembre de 2023].

²²⁹ A Strategic Compass for the EU. Disponible en: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en [Fecha de consulta: 03 de noviembre de 2023].

²³⁰ EU Strategic Compass for Security and Defence, p. 45

incremento defensivo de cada uno de los EEMM de forma individual. Es decir, la búsqueda de armonización presupuestal en seguridad y defensa dentro de la Unión deriva en el hecho de que los EEMM gocen de un estatus equivalente entre sí en esta materia.

Bajo este prisma comunitario de asociación e inversión, la PCSD facilita que la UE intervenga al unísono en el Sistema internacional coordinando esfuerzos en pro del objetivo común de garantizar la seguridad de la UE y de todos sus ciudadanos. Es precisamente esta visión de seguridad comunitaria y armonización²³¹ lo que define con precisión la Política Criminal de Europa.

En el desarrollo de la dimensión externa de su Política Criminal, la Unión Europea mantiene alianzas con socios estratégicos.

Sí bien actualmente existe cooperación en materia de seguridad con una gran mayoría de Estados, Organizaciones Internacionales y bloques regionales, con lo que se comparte una misma visión geopolítica, existen socios estratégicos, principalmente Estados Unidos de América y la OTAN, con los cuales se han adoptado unos compromisos en términos de reciprocidad que se orientan al sostenimiento de la seguridad internacional.

La relación actual UE-OTAN se basa en el principio de defensa colectiva. Este principio está consagrado en el artículo 5 del Tratado del Atlántico Norte²³², y estipula que un “ataque contra uno de los aliados se considerará un ataque contra todos los aliados”.²³³ Estos compromisos fueron adquiridos tempranamente y de forma individual por cada uno de los Estados europeos, antes de la existencia de la Unión Europea o de cualquier modelo de integración regional europeo.

El Tratado implica para cada aliado el compromiso con una alianza militar a fin de conectar recíprocamente la defensa de Estados Unidos con algunos Estados europeos sobre la base del artículo 51 (Capítulo VII) de la Carta de Naciones Unidas, en donde se reconoce el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado.

El principio de defensa colectiva, recogido en el artículo 5 en el Tratado del Atlántico Norte, detalla que:

«[Artículo 5]. Las partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte.

Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán inmediatamente en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de

²³¹ Armonización no solo en el ámbito presupuestal, sino también en materia judicial y policial, normativa, institucional, preventiva, democrática, investigación orientada a la seguridad y defensa, etc.

²³² La Organización del Tratado del Atlántico Norte (OTAN) se estableció en el año 1949. Conocido también como el Tratado de Washington, fue un modelo pionero de cooperación en materia defensiva. Los Estados firmantes (Bélgica, Canadá, Dinamarca, Estados Unidos, Francia, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal y Reino Unido) se obligaron a la defensa mutua en caso de agresión armada contra cualquiera de ellos. En más de setenta años de andadura, el principio de defensa colectiva ha sido invocado solo una vez, tras los ataques terroristas del 11 de septiembre de 2001 en suelo estadounidense.

²³³ «70 años de defensa colectiva», Ejército de Tierra, Ministerio de Defensa, Gobierno de España, lunes 3 de junio de 2019. Disponible en: https://ejercito.defensa.gob.es/gl/reportajes/2019/82_aniversario_otan.html [Fecha de consulta: 06 de noviembre de 2023].

Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales.»²³⁴

Para comprender mejor la importancia de esta alianza debemos remontarnos a la época en la que aún se estaba gestando la Unión Europea. Desde sus orígenes, los Estados europeos centraron su vigor colectivo en crear una fuerte alianza económica.²³⁵ Ello determinó en gran medida el futuro de la región durante los primeros años de su desarrollo, debido a que los EEMM de la época centraron todo su poderío en materia comercial, y aunque no en materia defensiva o de seguridad.²³⁶ Dicha situación significó que, de forma temprana, el bloque gestase acuerdos con aliados estratégicos que le aportasen estructuras de seguridad y defensa colectiva que la región europea aún no había desarrollado.

Recién en el año 1993, con la entrada en vigor del Tratado de Maastricht que habilitó la creación de la Unión Europea, los Estados Europeos adquieren una conciencia sobre su propia potencialidad como OOII en materia defensiva y de seguridad internacional.

Y es a partir de este momento y no antes, con el establecimiento de la PESC como segundo pilar fundacional de la UE, cuando comienzan todas las medidas, políticas y estrategias de seguridad y defensa común.

En este contexto histórico, de amplia integración estatal, se redacta el artículo 42.7 del Tratado de la Unión Europea. El mismo introduce la Cláusula de asistencia mutua por medio de la cual los EEMM se comprometen a la cooperación para la defensa mutua. El artículo 42.7, de conformidad con el artículo 51 de la Carta de las Naciones Unidas, faculta a que la UE brinde su ayuda y asistencia, con todos los medios a su alcance, si un EEMM es objeto de una agresión armada en su territorio.

Según De Castro Ruano, la Cláusula de asistencia mutua no ha estado exenta de debate debido a que:

«Esta cláusula levantó muchas suspicacias tanto en los países neutrales como en los atlantistas. Los primeros temían que mediante ella la Unión evolucionase hacia una alianza militar defensiva, pues lo que caracteriza a estas es, precisamente, el compromiso de defensa mutuo. Los segundos creían que esta cláusula podría dejar sin sentido al artículo 5 de la alianza atlántica. El intento de vencer este temor por parte de los socios comunitarios más atlantistas es lo que justificó la inclusión del segundo párrafo de este artículo 42.7: ‘Los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la OTAN, que seguirá siendo, para los Estados Miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de está’. Es decir, de alguna forma queda limitado el alcance de la defensa mutua por el carácter específico de cada Estado en materia de defensa y concretamente por los compromisos derivados de la pertenencia a la alianza atlántica. Idea

²³⁴ Tratado del Atlántico Norte. Disponible en: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=es [Fecha de consulta: 06 de noviembre de 2023]. El presente Tratado entró en vigor para España el día 30 de mayo de 1982, fecha del depósito del Instrumento de Adhesión de conformidad con lo dispuesto en su artículo 10: *“Las Partes pueden, por acuerdo unánime, invitar a adherirse al Tratado a cualquier otro Estado europeo que esté en condiciones de favorecer el desarrollo de los principios del presente tratado y de contribuir a la seguridad de la región del Atlántico Norte. Cualquier Estado así invitado puede pasar a ser parte en el Tratado depositando su instrumento de adhesión ante el Gobierno de los Estados Unidos de América. Este informará a cada una de las Partes del depósito de cada instrumento de adhesión.”*

²³⁵ Se hace referencia a la Comunidad Europea del Carbón y del Acero (CECA), a la Comunidad Económica Europea (CEE) y la Comunidad Europea de la Energía Atómica (CEEa), cuyos tratados establecían bases comunes de desarrollo estrictamente económico. Véase Índice: ANEXOS. Anexo N.º 01: *Origen y evolución de la Unión Europea*.

²³⁶ Tal desarrollo es completamente lógico a cualquier Organización Internacional, y responde a los grados o escalones de integración descriptos en el inicio del Capítulo 4. Ver: *Tabla 2. Nivel de integración regional de la Unión Europea*.

que, por otra parte, ya había quedado suficientemente explicitada en el último párrafo del artículo 42.2 ('la política de la Unión con arreglo a la presente sección no afecta al carácter específico de la política de seguridad y defensa de determinados Estados Miembros, respetará las obligaciones derivadas del tratado del atlántico Norte para determinados Estados Miembros que consideran que su defensa común se realiza dentro de la OTAN y será compatible con la política común de seguridad y defensa establecida en dicho marco').»²³⁷

Este debate parece indicar que los intereses de la Unión Europea por establecer sistemas propios de cooperación común en materia de seguridad y defensa, se observa con cautela por algunos Estados europeos y también por Estados Unidos, si ello supone un riesgo a los compromisos previos establecidos con la OTAN.

Hace más de veinte años, concretamente en septiembre de 2002, la Administración Bush estableció la Estrategia de Seguridad Nacional de EE.UU. La Estrategia de Seguridad Nacional estadounidense identificaba a la Unión Europea, junto a la OTAN, como una de las “dos instituciones internacionales más fuertes y capaces del mundo”, la relegaba a un papel de mero actor económico al calificarla en ese entonces como “nuestro socio en la apertura del comercio mundial.”²³⁸ Ante esta declaración, Europa manifestó la necesidad de elaborar un *concepto estratégico* con el que responder a la estrategia Bush. En el año 2003, en el marco de la Asamblea de la Unión Europea Occidental (UEO) se reconoce que la UE había sido incapaz hasta esa fecha de “establecer un concepto estratégico que pudiese proporcionar un enlace con el de los Estados Unidos, para así fortalecer la cooperación transatlántica sobre seguridad internacional”. Dicha Asamblea determinó que el vínculo transatlántico seguía siendo “el elemento central de la seguridad y defensa europea”, pero debía “ser utilizado en beneficio de todas las partes.”²³⁹

A pesar de la respuesta de la Asamblea, la UE continúa enclavada en gran medida al poderío económico que determinó la génesis de su origen y posterior desarrollo. Aun cuando esto ha sido siempre un gran valor, ha significado en gran medida que su actual injerencia en el Sistema internacional se encuentre lastrada a dicho origen.

Sí bien el presente dista mucho de la célebre afirmación esgrimida por el ministro belga de Asuntos Exteriores, quien definió a Europa como “un gigante económico, un enano político y un gusano militar”²⁴⁰, existe aún una gran porción de Estados europeos que poseen una percepción frágil de la UE en materia de seguridad y defensa.

La visión actual de EE.UU. sobre la UE en esta línea puede encontrarse en su nueva Estrategia de Seguridad Nacional (ESN), vigente desde el 12 de octubre de 2022 y establecida por la Administración Biden. En la ESN de 2022 EE.UU. relega a un segundo plano la atención hacia la UE, por centrar su mayor atención en la región Indo-Pacífico.

Según Simón y García Encina,

«Esta asunción revierte en un mayor apoyo a la autonomía europea, tal y como avalan las referencias de la ESN a las inversiones europeas en defensa ‘a través de la OTAN o de forma complementaria a ella para

²³⁷ DE CASTRO RUANO, José Luis (2015), opus cit., p. 32.

²³⁸ THE WHITE HOUSE (2002): *The National Security Strategy of the United States of America*. Washington, September 2002, p. 25.

²³⁹ THE INTERPARLIAMENTARY EUROPEAN SECURITY AND DEFENCE ASSEMBLY (2003): *Assembly of Western European Union. Recommendation 726, on the United States National Security Strategy and its consequences for European defence*, adopted unanimously by the Assembly without amendment on 4 June 2003 (4th sitting).

²⁴⁰ La declaración, pronunciada en 1991, pertenece a Mark Eyskens exministro de Asuntos Exteriores de Bélgica.

garantizar la seguridad compartida’.²⁴¹ Si bien estas afirmaciones parecen confirmar el apoyo de EEUU a una mayor autonomía europea en el ámbito de la defensa, incluido el industrial, las referencias a la complementariedad con la OTAN siguen planteando dudas sobre el grado de autonomía europeo que la Administración Biden estaría dispuesta a aceptar.»²⁴²

Esta visión sobre el modelo defensivo de una Unión Europea dependiente en extremo de la OTAN es valorada por EE.UU. y por algunos EEMM de la Unión y, debido a ello, prevalece en la actualidad una percepción sobre el poder²⁴³ que ostenta cada uno. Existen, sin embargo, voces contrarias a esta opinión. De acuerdo con De Castro Ruano:

«El empleo de la fuerza militar no constituye la única opción y, en muchas ocasiones, puede resultar contraproducente; pero en otras muchas, es imprescindible. Dependerá de las condiciones específicas de cada conflicto la pertinencia o no de utilizar uno u otro de los recursos existentes, ya sean de naturaleza civil y/o militar. Frente a la recurrente caracterización de la UE como Venus y EE.UU. como Marte²⁴⁴, actualmente la Unión tiene que ser Venus y Marte a la vez. La clave hoy en día no reside en la utilización del poder duro o del blando, sino en utilizar aquel poder más adecuado para enfrentar las circunstancias concretas que los distintos escenarios internacionales requieren: el poder ‘inteligente’.»²⁴⁵

Una muestra evidente de que la Unión Europea desarrolla también acciones tendientes a acrecentar su *poder duro* es la creación de Agrupaciones Tácticas de Reacción Rápida (*EU Battlegroups*).²⁴⁶

En el Consejo Europeo de Bruselas, celebrado en el año 2004, se redactó el *Objetivo Global 2010*.²⁴⁷ En este documento se menciona la creación de las Agrupaciones Tácticas de Reacción Rápida. Tales Agrupaciones han sido creadas teniendo en cuenta la existencia previa y a semejanza de la Fuerza de Reacción Rápida de la OTAN (*NRF, NATO Response Force*).

²⁴¹ US DEPARTMENT OF DEFENSE (2022): *2022 National Defense Strategy of the United States of America, including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*, Washington DC, 27/X/2022., p. 39. Como se citó en: SIMÓN, Luis/GARCÍA ENCINA, Carlota (2022): «La nueva Estrategia de Seguridad Nacional de EEUU», *Real Instituto Elcano ARI 69/2022*, 8 de noviembre de 2011, p. 2.

²⁴² BERGMANN, Max (2022), “Europe on its own: why the United States should want a better-armed EU”, *Foreign Affairs*, 22/VIII/2022. Como se citó en: *Ibidem*, p. 4

²⁴³ El concepto de ‘poder’ se aplica aquí según la Teoría de Realismo Clásico de Hans Morgenthau, propia de las Relaciones Internacionales, por la cual se explica que el poder de un Estado está determinado por su capacidad armamentística, sin tener en cuenta consideraciones de tipo moral o político. Según el Realismo Clásico obtener, mantener y consolidar el poder, por encima de otros actores internacionales, es el único fin del Estado.

²⁴⁴ KAGAN, Robert (2003). *Poder y debilidad. Europa y Estados Unidos en el nuevo orden mundial*. Madrid: Santillana. Como se citó en: DE CASTRO RUANO, José Luis (2015), opus cit., pp. 19-48.

²⁴⁵ Según De Castro Ruano, “*El paradigma aplicable a la acción exterior de la UE actualmente es el de Smart Power o «poder inteligente», para referirse no precisamente a un punto intermedio entre poder civil y militar, sino a la combinación más adecuada de poder, duro y/o blando, civil y/o militar. Es decir, todo el conjunto de instrumentos de acción exterior a disposición: diplomáticos, económicos, políticos, legales, culturales y, también militares. Se trata de elegir el instrumento más adecuado, o la combinación de ellos, para enfrentar cada situación. Es un concepto más cercano al de poder civil, aunque añadiéndole también la dosis necesaria de poder militar cuando sea menester.*” *Ibidem*, p. 24-25. El autor referencia dos textos para comprender mejor este concepto desde una aplicación europea: CEBADA ROMERO, Alicia (2008): *La Unión Europea: ¿una acción exterior inteligente?*, Madrid: Iustel.; y, desde una aplicación estadounidense: CHARMELOT, Jacques (2009): «Le Smart Power Américain, un défi pour l’Europe», *Questions d’Europe*, N.º 127.

²⁴⁶ Las Agrupaciones Tácticas, también conocidas como Grupos de combate de la UE, están compuestas por unos 1500 integrantes (pudiendo llegar hasta 4.000 efectivos sumando los grupos especializados para transporte y logística), y deben ser capaces de desplegarse sobre el terreno en un plazo máximo de 10 días desde la aprobación de la decisión de su uso, y tener la capacidad de mantenerse de forma autónoma en el epicentro de operaciones en un plazo de entre 30 y 120 días. Las Agrupaciones Tácticas iniciaron su actividad de forma reducida en el año 2005 y alcanzaron su capacidad operativa plena a partir del año 2007.

²⁴⁷ EUROPEAN COUNCIL (2004): *Headline Goal 2010*. Approved by General Affairs and External Relations Council on 17 May 2004 endorsed by the European Council of 17 and 18 June 2004. (Documento en inglés). Disponible en: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede110705headlinegoal2010_/sede110705headlinegoal2010_en.pdf [Fecha de consulta: 09 de noviembre de 2023].

Las Agrupaciones Tácticas de Reacción Rápida de la UE son dos grupos de combate multinacionales con capacidad operativa de emergencia que pueden activarse ante cualquier crisis o amenaza. Cada uno de estos dos grupos de combate están integrados cada semestre por diferentes EEMM de la Unión.²⁴⁸ Esta rotación determina también el Estado Base (Estado Miembro que lidera cada grupo) donde se ubica el Cuartel General operativo.

El artículo 43 del TUE recoge todos los escenarios en los cuales pueden emplearse las Agrupaciones Tácticas. Entre ellas, contempla la prevención de conflictos, fases de estabilización inicial, intervenciones humanitarias y de rescate, gestión de crisis o misiones de paz. De acuerdo con la PCSD, para su activación e intervención en cualquiera de estas situaciones se requiere la aprobación por unanimidad del Consejo de la UE.

Las Agrupaciones Tácticas no son un ejército europeo, pero representan en cierta forma la antesala de una idea que resuena cada vez con más fuerza en Bruselas: la creación de un ejército europeo propio. Josep Borrell, alto representante para Asuntos Exteriores y Política de Seguridad, sostiene que este tipo de medidas orientadas a la militarización y distanciadas del *Soft power*²⁴⁹ podría enseñarle a Europa a "hablar el lenguaje del poder".²⁵⁰

A partir del año 2021 Borrell comenzó a referirse reiteradamente a la autonomía estratégica de la Unión Europea²⁵¹. En diversas declaraciones detalló que la Unión debía de crear su propia fuerza militar, a fin de terminar con la "alarmante dependencia europea del poderío militar estadounidense".²⁵² Dos años antes, concretamente en noviembre de 2019, la Presidenta electa de la Comisión Europea, Ursula von der Leyen²⁵³, destacó durante el discurso de presentación de su Ejecutivo ante el Parlamento Europeo, la necesidad de tener una Europa más fuerte. Von der Leyen expresó "Esta [en referencia a fortalecer la seguridad y defensa europea a través de la cooperación militar] es la Comisión geopolítica que tengo en mente y que Europa necesita de manera urgente".²⁵⁴

Durante los últimos diez años, uno de los ejes centrales de la Política Criminal de la UE es la lucha contra el terrorismo internacional, con especial foco estratégico en la lucha contra el terrorismo yihadista global. Para llevar adelante esta lucha, la UE se apoya en la PESC-PCSD a fin de estimular la mayor armonización y cooperación posible entre todos los EEMM que

²⁴⁸ España liderará un contingente en el segundo semestre de 2022.

²⁴⁹ *Soft power* o Poder blando es un concepto propio de las Relaciones Internacionales que ha sido acuñado y ampliamente difundido por Joseph Nye. Implica la ponderación de un Estado (u otro actor político) dentro del Sistema internacional con independencia de su capacidad armamentística. Entiende el poder como la capacidad de un actor para influir en otros actores valiéndose de recursos persuasivos cimentados en medios culturales, ideológicos y/o diplomáticos. Véase: NYE, Joseph. (2004): opus cit.

²⁵⁰ BORRELL, Josep (2020). «Europa debe aprender rápidamente a hablar el lenguaje del poder. / Entrevistado por J. H. H. Weiler», *Periódico El País*. Disponible en: <https://agendapublica.elpais.com/noticia/16744/borrell-europa-debe-aprender-rapidamente-hablar-lenguaje-poder> [Fecha de consulta: 09 de noviembre de 2023].

²⁵¹ Conocida coloquialmente como *Autonomía Estratégica de los 27*.

²⁵² «Por qué la Unión Europea no tiene un ejército propio y qué son los 'battlegroups' de la UE», *AS España*, edición online de 28 de febrero de 2022. Disponible en: https://as.com/diarioas/2022/02/28/actualidad/1646032381_346464.html [Fecha de consulta: 09 de noviembre de 2023].

«Borrell pide una fuerza militar de la UE: "Estados Unidos ya no hará las guerras de los demás», *El Confidencial*, Disponible en: https://www.elconfidencial.com/mundo/europa/2021-08-22/borrell-critica-que-eeuu-hace_3244478/ edición online de 23 de agosto de 2021. [Fecha de consulta: 09 de noviembre de 2023].

²⁵³ Cercana ideológicamente a Borrell con su visión de la seguridad y defensa europea.

²⁵⁴ Discurso ante la sesión plenaria del Parlamento Europeo (2019): *Discurso pronunciado por Ursula von der Leyen, Presidenta electa de la Comisión Europea*, 27 de noviembre de 2019, p. 7. Disponible en: https://commission.europa.eu/system/files/2019-11/president-elect-speech_es.pdf [Fecha de consulta: 09 de noviembre de 2023].

permita una persecución eficaz del terrorismo dentro y fuera de la UE. Sin embargo, esta empresa presenta problemas que amenazan la propia coordinación de la UE en materia de seguridad y defensa. Arribar, por ejemplo, a un ejército común europeo parece inaccesible, aunque resultaría estratégicamente muy conveniente.

El proyecto de un Ejército común no es algo nuevo, de hecho, data de inicios de la EU. Lo reseñable y novedoso de los últimos años son los apoyos de un mayor número de EEMM que se han sumado recientemente a impulsar este proyecto. No obstante, este proyecto no está exento de algunos problemas que pueden ser anticipados en menor o mayor medida conforme a la evaluación objetiva de las actuales Agrupaciones Tácticas de Reacción Rápida de la UE.

En la actualidad, las Agrupaciones Tácticas de Reacción Rápida enfrentan problemas de financiación. Los costos de entrenamiento y establecimiento de los grupos de combate son responsabilidad de los propios EEMM participantes. Este impacto en el presupuesto de cada Estado, aunado al hecho de que la participación en las Agrupaciones Tácticas no es obligatoria sino voluntaria, trae como consecuencia que cada vez existan mayores dificultades para completar los batallones con el número mínimo de efectivos requeridos.²⁵⁵

Además, de cara a la creación de un ejército común europeo, otro de los posibles problemas que permite anticipar el actual funcionamiento de las Agrupaciones Tácticas, es que los EEMM tienen dificultades para integrar los batallones debido a que ya tienen comprometidas parte de sus tropas con la OTAN.

Si bien las Agrupaciones Tácticas han resultado un logro que ha ayudado a implementar técnicas de entrenamiento común europeo y a establecer procedimientos de certificación militar²⁵⁶, también han evidenciado la compleja y delicada que resulta la integración europea en materia de seguridad y defensa. La Política Criminal de la Unión se ve por tanto atravesada por esta ardua tarea de equilibrar los intereses de la UE con las limitaciones de los EEMM. Debido a este complejo escenario, la Política Criminal de la UE se ha centrado, lejos de las tensiones presupuestarias, en buscar puntos de referencia común entre todos los EEMM en el ámbito normativo, policial y judicial, y preventivo, proponiendo la armonización de estos aspectos en todos los territorios nacionales a fin de que redunde en beneficio de la Unión.

²⁵⁵ Este dato es significativo en cuanto actualmente las agrupaciones tácticas de reacción rápida se encuentran integradas por unos 1500 efectivos aproximadamente, un número muy pequeño. Un ejército europeo debería de poder integrar tropas de militares de unos 5000 efectivos, a fin de poder actuar de forma independiente a Estados Unidos. En síntesis, ante las mismas condiciones presupuestarias, la dificultad para completar los batallones se triplicaría con un ejército común. “*Por ello se creó el nuevo Fondo Europeo de Apoyo a la Paz el año pasado, con un presupuesto de 5.000 millones de euros para el periodo 2021-2027*”. Véase: «Por qué la Unión Europea no tiene un ejército propio y qué son los 'battlegroups' de la UE», *AS España*, edición online de 28 de febrero de 2022. Disponible en: https://as.com/diarioas/2022/02/28/actualidad/1646032381_346464.html [Fecha de consulta: 13 de noviembre de 2023].

²⁵⁶ Dichas certificaciones las otorga el Cuartel General de la OTAN para operaciones especiales (NSHQ) y permite, una vez obtenida, que la Agrupación Táctica certificada trabaje juntamente con la NRF (*Nato Response Force*) en el teatro de operaciones designado. Para la obtención de dicha certificación se requiere de un entrenamiento especial, cuyas características pueden encontrarse en la editorial a continuación. En ella se describe un entrenamiento y simulación de la Aviación Militar española bajo el supuesto de secuestro de cooperantes internacionales por parte de un grupo terrorista. Véase: «El Ejército del Aire reúne en Canarias a 2.000 militares y 35 aeronaves en su principal ejercicio del año», *Revista Mundo militar Infodefensa*, edición online de 19 de octubre de 2022. Disponible en: <https://www.infodefensa.com/texto-diario/mostrars/3930922/ejercito-aire-espacio-da-comienzo-ejercicio-otan-sirio-22> [Fecha de consulta: 13 de noviembre de 2023]. Véase: «Nuestras unidades de operaciones aéreas especiales: helicópteros, paracaidistas y mucho más», *Aviación militar*, edición online de 19 de junio de 2023. Disponible en: <https://aviacionmilitar.es/nuestras-unidades-de-operaciones-aereas-especiales-helicopteros-paracaidistas-y-mucho-mas> [Fecha de consulta: 13 de noviembre de 2023]. Véase: «Grupo táctico de operaciones aéreas especiales para la Fuerza de Respuesta Rápida de la OTAN», *Ministerio de Defensa*. Disponible en: <https://ejercitodelaire.defensa.gob.es/EA/ejercitodelaire/es/noticias/noticia/Grupo-tactico-de-operaciones-aereas-especiales-para-la-Fuerza-de-Respuesta-Rapida-de-la-OTAN/> [Fecha de consulta: 13 de noviembre de 2023].

La UE aplica esta armonización en la lucha contra el terrorismo yihadista, y lo hace por medio de tres vías muy definidas: por medio de la vía normativa, a través de la institucionalización de la cooperación policial y judicial, y por medio de enfoques conceptuales y/o preventivos de alerta temprana. Todo ello está orientado a frenar el terrorismo en Europa y le permite a la Unión Europea prevenir, reprimir y sancionar este delito.

Hacia el análisis de estos tres elementos, que le son propios a cualquier Política Criminal, se orientará nuestro estudio en los siguientes capítulos. Para ello, se desarrollará una revisión normativa en diferentes niveles, a fin de sintetizar los instrumentos con los que se cuenta al presente la Unión Europea para luchar contra el terrorismo yihadista, y especialmente el terrorismo yihadista en Internet. Ello nos llevará a compilar la normativa de la Unión Europea, reseñando sus Decisiones marco, Decisiones UE y Directivas más relevantes en la materia. También se revisará la normativa en la materia del Consejo de Europa, y la influencia que tiene y ha tenido el derecho internacional en la región.

Además, se analizará la institucionalización de la cooperación policial y judicial europea destinada a reprimir y neutralizar las acciones en Internet de los grupos yihadistas, priorizando un enfoque operativo y criminológico sobre la visión jurídica de revisión normativa en la materia. Mediante un análisis descriptivo se explicará la creación de centros especializados para la investigación de este fenómeno, la coordinación europea en el ámbito policial y judicial, el intercambio de información, y el control de las fronteras exteriores de la Unión.

Por último, se describirán los enfoques conceptuales y/o preventivos de alerta temprana que la Unión Europea desarrolla actualmente o ha desarrollado con anterioridad con el objeto de detectar y prevenir nuevas captaciones o posibles radicalizaciones yihadistas dentro de la Unión. El estudio de estos capítulos (uno por cada elemento de la Política Criminal europea) nos permitirá comprender si la implementación de los mismos facilita o no la superación de las tensiones internas de la Unión que amenazan la consolidación de la seguridad común de la región.

CAPÍTULO 5: MEDIDAS NORMATIVAS EUROPEAS ORIENTADAS A LA PERSECUCIÓN DEL USO DE INTERNET CON FINES YIHADISTAS

EL DERECHO DE LA UNIÓN EUROPEA COMO ORDENAMIENTO JURIDICO PROPIO

Dentro de las medidas de contraterrorismo adoptadas por la Unión Europea y que son constitutivas de su Política Criminal, nos encontramos en primera instancia con las medidas normativas.

Ello es así porque las medidas normativas han sido el primer elemento de desarrollo de la Política Criminal europea, y estas paulatinamente han ido creciendo hasta establecerse en un ordenamiento jurídico propio.

El ordenamiento jurídico de la Unión Europea se conoce como DUE (Derecho de la Unión Europea), y comprende los Tratados constitutivos del llamado Derecho originario o Derecho primario de la UE, junto a los Principios generales del Derecho; y el Derecho producido por la UE, conocido este último como Derecho derivado o Derecho secundario de la UE. El Derecho derivado o secundario es elaborado por la Unión Europea a través de sus instituciones o bien a través de acuerdos con EEMM.

La UE también es productora de Derecho internacional. Este Derecho internacional se haya contemplado en una categoría jurídica externa al Derecho primario y secundario, y se elabora mediante acuerdos con terceros Estados,²⁵⁷ u otras Organizaciones Internacionales.

Sí bien desde un punto de vista estrictamente criminológico el análisis doctrinario de la legislación europea puede ser observado como prescindible, resulta un elemento clave y valioso para comprender el posicionamiento de la Unión frente al fenómeno del terrorismo. La adopción de medidas normativas nos permite valorar no solo las consideraciones generales del ordenamiento jurídico europeo, sino también la ideología²⁵⁸ que sustenta la Política Criminal de la Unión en relación con el terrorismo yihadista. Aspectos como el régimen sancionador, la existencia o no de sanciones alternativas a la prisión, el régimen penitenciario, etc., son fundamentales para comprender qué es lo que “piensa” la Unión Europea respecto al terrorismo yihadista, y a su vez cómo se posiciona frente a este.

El análisis del Derecho de la UE, además de documentarnos respecto de la ideología que promueve su Política Criminal, nos permite analizar en detalle cuál es la normativa europea que se ha desarrollado en la lucha contra el terrorismo yihadista. Este Derecho, específico a la materia del terrorismo yihadista, es fundamental debido a que es el que regula la cooperación

²⁵⁷ Tercer Estado implica un posicionamiento de un Estado (fuera de) respecto de la Unión Europea. En relación con la Unión Europea se denomina ‘Tercer Estado’ a cualquier Estado del Sistema internacional que no pertenezca a la Unión en el momento de aplicación del término. Este concepto tiene su origen en el feudalismo. Antes del surgimiento en el S. XIX del Estado moderno, la sociedad feudal se encontraba dividida en estamentos. La nobleza, el clero, los soldados y los siervos de gleba formaban parte del sistema feudal de la época. A su vez existía un campesinado libre y una incipiente burguesía europea. Ambas (campesinado libre y burguesía) se encontraban al margen de la estructura estamental de la época y debido a ello se les concedió el nombre de Tercer Estado o Tercer Estamento. El Tercer Estado se encontraba libre de las obligaciones del sistema feudal, pero también se hallaba carente de los privilegios que otorgaba el mismo. El término ‘Tercer Estado’ remite, por tanto, en la actualidad, a la no pertenencia a un sistema que posea una organización jurídica propia.

²⁵⁸ Nos referimos aquí a la ideología que se ha descrito en el CAPÍTULO 4: LA POLÍTICA CRIMINAL DE LA UE ANTE EL YIHADISMO ONLINE, en la que se enunciaba que toda Política Criminal de un Estado está compuesta previamente por una ideología sustentadora.

policial y judicial institucionalizada, hacia dentro y hacia fuera de la Unión, actuando como un ordenamiento jurídico propio.

El Derecho de la Unión actúa como un ordenamiento jurídico propio en el sentido de que no solo es una conjunción de normas y principios, sino que es un conjunto destinado a la obtención de determinados objetivos (comunes a todos los EEMM y específicos a una materia), con reglas y procedimientos de elaboración y aplicación propios, todo ello conforme a los valores de la Unión, y a su vez dentro de los límites que establecen los tratados fundacionales de la UE. Este hecho ha sido desde un inicio de suma importancia para el funcionamiento de la Unión, de tal forma que tempranamente ha intentado definir y sentar las bases de los ámbitos materiales en los que la Unión posee competencias.²⁵⁹

Para el logro de objetivos comunes y específicos a la lucha contra el terrorismo, la UE se vale de su Derecho derivado. Dentro del Derecho derivado encontramos una serie de instrumentos normativos²⁶⁰ que permiten la coexistencia de todo un acervo jurídico en la materia específica. Por tratarse del interés de este estudio, nos enfocaremos de ahora en más en el Derecho derivado de la UE con relación al terrorismo y específicamente al terrorismo en Internet, analizando con especial atención Decisiones, Directivas de la UE y Acuerdos relativos a este fenómeno. Esta especial atención a estos tipos de instrumentos jurídicos es debido al hecho de que son aquellos que han propiciado el mayor crecimiento normativo en la lucha contra el yihadismo.

El Derecho derivado, por tanto, es aquel que ha permitido pasar de una cooperación espontánea hacia una cooperación sistematizada entre instituciones y agencias (cooperación interinstitucional vertical y horizontal), entre instituciones/agencias y EEMM (cooperación vertical) y entre los propios EEMM (cooperación horizontal).

El Derecho de la UE fomenta la cooperación policial y judicial entre diversos actores de la Unión Europea. La cooperación vertical y horizontal dentro de la Unión tiene lugar entre instituciones y agencias de la UE. Se trata de una cooperación interinstitucional que se da entre sí y que facilita, por ejemplo, el intercambio de información y el desarrollo de actividades coordinadas entre dos o más instituciones o agencias. Encontramos también dentro de la UE una cooperación exclusivamente vertical que tiene lugar entre las instituciones y/o agencias de la UE con los EEMM, y viceversa. Esta cooperación vertical habitualmente promueve el intercambio de información entre ambas partes. Finalmente, existe la cooperación que tiene lugar entre los EEMM entre sí. Esta cooperación no solo promueve el intercambio de información en material policial y judicial (por ejemplo, propiciando el reconocimiento mutuo

²⁵⁹ Las sentencias *van Gend & Loos* y *Flaminio Costa*, emitidas por el Tribunal de Justicia (Tribunal de Justicia de la Unión Europea, TJUE) en el año 1963 y 1964 respectivamente, evidencian que con solo un año de diferencia el TJUE ha pasado de afirmar que el DUE es un “nuevo ordenamiento jurídico de Derecho Internacional” a enunciar que el DUE constituye un “ordenamiento jurídico propio.” Ambas sentencias disponibles en: *Sentencia del Tribunal de Justicia de 5 de febrero de 1963. NV Algemene Transport-en Expeditie Onderneming van Gend & Loos contra Administración fiscal holandesa.* <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C.T.F&num=26/62&td=ALL> [Fecha de consulta: 16 de noviembre de 2023]. *Sentencia del Tribunal de Justicia de 15 de julio de 1964. Flaminio Costa contra E.N.E.L. Petición de decisión prejudicial: Giudice conciliatore di Milano - Italia. Asunto 6-64.* <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:61964CJ0006> [Fecha de consulta: 16 de noviembre de 2023].

²⁶⁰ Nos referimos a los instrumentos con los que cuentan las instituciones europeas para la realización de su misión. Estos instrumentos se encuentran detallados en el artículo 288 del Tratado de Funcionamiento de la Unión Europea (TFUE), y son: 1) el Reglamento: obligatorio y directamente aplicable en cada Estado Miembro; 2) la Directiva: obliga al EEMM a la obtención de determinados resultados. Requiere de una transposición al ordenamiento jurídico nacional de cada Estado, y otorga libertades en cuanto a la forma y los medios de su aplicación; 3) la Decisión: obligatoria en todos sus elementos, vincula a los destinatarios a quienes designa expresamente; y, 4) la Recomendación y el Dictamen: no obligatorios, posee únicamente carácter declaratorio.

de sentencias judiciales), sino que también adopta la forma de acuerdos específicos para un objetivo concreto. Esto último se conoce como Cooperación reforzada, y consiste en que, mediante un acuerdo *ad hoc*, un grupo de EEMM trabaje de forma voluntaria entre sí en una materia específica. No solo el Derecho de la UE promueve esta forma de cooperación, sino que, a su vez, la producción normativa que tenga lugar dentro de la Cooperación reforzada acaba finalmente siendo adoptada por las instituciones de la Unión.²⁶¹

Antes de adentrarnos en el análisis específico de instrumentos normativos que den cuenta de nuestro objeto de estudio, estableceremos una aclaración respecto a las Decisiones y Directivas, dos instrumentos del Derecho derivado, a fin de entender la importancia del alcance y la fuerza jurídica de cada modalidad normativa dentro de la Unión. Las Decisiones que analizaremos son de dos tipos: Decisiones marco (DM) y Decisiones de la UE. La Decisión Marco es un acto legislativo de la Unión Europea con competencias únicamente comunitarias que se utilizan en el ámbito de cooperación policial y judicial en materia penal. El fundamento jurídico de las DM se encuentra en el artículo 34.2 del derogado Tratado de la Unión Europea:

«El Consejo dispondrá y fomentará, en la forma y según los procedimientos oportunos tal como se establece en el presente título, la cooperación pertinente para la consecución de los objetivos de la Unión. A tal fin, a iniciativa de cualquier Estado Miembro o de la Comisión, el Consejo podrá, por unanimidad: [...] b) adoptar decisiones marco para la aproximación de las disposiciones legales y reglamentarias de los Estados Miembros. Las decisiones marco obligarán a los Estados Miembros en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.»²⁶²

Las DM han sido sustituidas por las Decisiones de la UE a partir de la entrada en vigor en el año 2009, del Tratado de Lisboa. No obstante, el propio Tratado de Lisboa recoge en su artículo 9, que se mantendrán los efectos jurídicos de las DM elaboradas por instituciones, órganos y organismos de la Unión antes de su entrada en vigor.²⁶³ Esto explica que en nuestro análisis encontraremos Decisiones marco y Decisiones de la UE, mismo tipo de instrumento normativo, antes y después del Tratado de Lisboa. Por otro lado, analizaremos Directivas orientadas a la lucha contra el terrorismo. Las Directivas son actos legislativos mediante los cuales se determinan objetivos que todos los Estados de la UE deben cumplir.²⁶⁴ No obstante, corresponde a las autoridades competentes de cada EEMM elaborar sus propias leyes para el logro de dichos objetivos. Habitualmente esta particularidad está sujeta a un condicionamiento presupuestario de cada EEMM, y de ello derivan las diferencias entre los EEMM para abordar un mismo problema. Las Directivas requieren de un complemento normativo por parte de los Estados para su implementación definitiva, que se denomina jurídicamente transposición al Derecho interno o nacional. Por tanto, “las Decisiones son vinculantes para aquellos a quienes se dirigen (un

²⁶¹ El Derecho derivado de cooperación reforzada no será vinculante para aquellos Estados que no hayan participado de dicha Cooperación reforzada.

²⁶² Artículo 34.2. TUE.

²⁶³ En el Tratado de Lisboa, en su artículo 9 del Protocolo (n.º 36), se detalla expresamente que: “Los efectos jurídicos de los actos de las instituciones, órganos y organismos de la Unión adoptados en virtud del Tratado de la Unión Europea antes de la entrada en vigor del Tratado de Lisboa se mantienen en tanto dichos actos no hayan sido derogados, anulados o modificados en aplicación de los Tratados. Lo mismo ocurre con los convenios celebrados entre los Estados Miembros sobre la base del Tratado de la Unión Europea.”

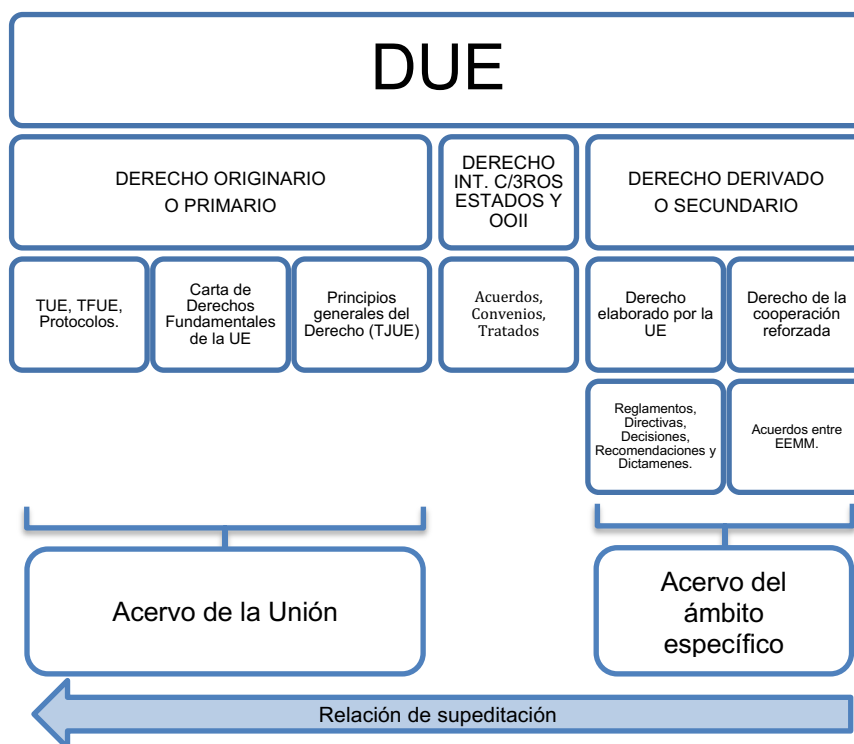
²⁶⁴ El incumplimiento (por transposición incorrecta, por su no transposición, o por transposición fuera del plazo previsto) hace al Estado infractor incurrir en responsabilidad ante la autoridad comunitaria ejecutiva (Comisión) y judicial (Tribunal de Justicia), que podrán imponer medidas coercitivas.

EEMM, una empresa europea, etc.) y son directamente aplicables.”²⁶⁵ Es en esta aplicación en donde la Unión Europea busca la mayor armonización posible en las legislaciones internas, a fin de lograr una Política Criminal común.

Las Decisiones (Decisiones marco que existían antes del Tratado de Lisboa, y las Decisiones de la Unión) tienen semejanza con las Directivas en el hecho de que exigen a los EEMM que logren determinados resultados sin indicar que medios deben emplearse para hacerlo. Sin embargo, a diferencia de las Directivas y de las actuales Decisiones de la Unión, las Decisiones marco carecían de efecto directo.²⁶⁶ Como se observa, las modificaciones normativas que introdujo el Tratado de Lisboa han redundado en beneficio de la actual cooperación policial y judicial de la Unión debido a la directa e inmediata aplicación de las Decisiones de la UE. Así, junto con las Directivas y los Acuerdos internacionales o los derivados de la Cooperación reforzada, constituyen la primera línea defensiva de la Política Criminal de la UE.

En un reduccionismo extremo, orientado a nuestro objeto de estudio, podemos graficar el actual ordenamiento jurídico de la UE de la siguiente manera:

Gráfico 5: Ordenamiento jurídico propio de la Unión Europea.



Fuente: Elaboración propia. 2023.

²⁶⁵ Tipos de legislación de la Unión Europea. Disponible en: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_es [Fecha de consulta: 16 de noviembre de 2023].

²⁶⁶ El efecto directo constituye un principio básico del derecho de la Unión. Dicho principio crea derechos a favor de los particulares para que puedan alegarlos ante los órganos jurisdiccionales nacionales y comunitarios. El efecto directo es un principio jurisprudencial sentado por el Tribunal de Justicia de la Unión Europea en la sentencia *van Gend & Loos*, 1963. No obstante, el Tribunal acepta hasta el momento únicamente el llamado efecto directo vertical (relaciones entre particulares y administraciones), pero no ha reconocido aún el efecto directo horizontal (relaciones entre particulares).

Esto nos permite determinar dónde se encuentra ubicado el Derecho derivado dentro del DUE y la relación de supeditación que guarda con el Derecho primario u originario.

Habiendo categorizado el Derecho de la Unión Europea, nos centraremos de ahora en adelante en el análisis del Derecho derivado de la Unión y las influencias del Derecho internacional (categoría independiente *sui generis* debido a que se encuentra excluida del Derecho primario y secundario de la Unión) con relación al terrorismo yihadista, y al terrorismo yihadista en Internet.

DERECHO DE LA UNIÓN EUROPEA REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS

En diciembre de 2003, la Unión Europea adoptó la Estrategia Europea de Seguridad, que se ocupa de la dimensión exterior de la seguridad de Europa.

En el marco de esta estrategia se adopta la ‘Estrategia de Seguridad Interior de la Unión Europea. Hacia un modelo europeo de seguridad’, elaborado por la Secretaría General del Consejo. Conforme al documento se reconoce que entre los principales riesgos y amenazas actuales para la seguridad de Europa se encuentran:

«[...]... el terrorismo, la delincuencia organizada y grave, el tráfico de drogas, el cibercrimen, la trata de seres humanos, la explotación sexual de menores y la pornografía infantil²⁶⁷, la delincuencia económica y la corrupción, el tráfico de armas y la delincuencia transfronteriza, cuyas acciones criminales se adaptan muy rápidamente a la evolución científica y tecnológica.»²⁶⁸

La Estrategia de Seguridad Interior de la Unión Europea se propone dar respuesta a esta gran variedad de crímenes por medio de la vía normativa, de enfoques conceptuales de prevención, y por medio de la cooperación policial y judicial.²⁶⁹ Como hemos dicho en reiteradas oportunidades, es la vía normativa, la primera medida que se adopta y en donde se centran todos los esfuerzos comunitarios. En este escenario es “el Tratado de Lisboa y el Programa de Estocolmo [los que] permiten que la Unión Europea pueda adoptar medidas ambiciosas y concertadas en el desarrollo de Europa como un Espacio de libertad, seguridad y justicia.”²⁷⁰

²⁶⁷ Cabe señalar que dicho documento fue elaborado en el año 2010 y que el concepto de ‘pornografía infantil’ era contemporáneo a la época. Actualmente ha dejado de utilizarse debido a que esta denominación no resulta en absoluto correcta, debido a que la producción de pornografía, así como el desarrollo de la industria pornográfica, supone una actividad entre adultos y consensuada entre todas las partes. Lo que tradicionalmente se ha conocido como ‘pornografía infantil’, no solo no reúne estas dos condiciones necesarias, sino que incluso oculta el hecho de que realmente se está ante la producción audiovisual de un abuso sexual infantil. Véase: pie de página N.º 74.

²⁶⁸ CONSEJO EUROPEO (2010): Estrategia de Seguridad Interior de la Unión Europea. Hacia un modelo europeo de seguridad. Luxemburgo: Oficina de publicaciones de la Unión Europea; p. 7.

²⁶⁹ Un ejemplo ilustrativo de esto es que, en el año 2007, a través de Eurojust, veintiséis personas en Francia, Italia, Portugal Reino Unido y Rumanía fueron detenidas en una operación contra el terrorismo. La organización tenía la intención de cometer atentados en Italia, Afganistán, Irak y los países árabes. Véase: EUROJUST (2007): *Informe anual 2007*, de enero de 2008, p. 34-35.

²⁷⁰ El Espacio de libertad, seguridad y justicia (ELSJ) se encuentra descrito en el Título V del Tratado de Funcionamiento de la Unión Europea (TFUE). El ELSJ establece el proceder de la UE, dentro y fuera de sus fronteras, para lograr el objetivo de crear un espacio en donde sus EEMM se alcancen un alto grado de cooperación y coordinación política, policial y judicial que promueva la seguridad interior, la justicia eficaz y una fuerte protección de las libertades ciudadanas. El ELSJ establece un espacio europeo sin control de fronteras interiores, a fin de promover la libre circulación de personas, a la vez que fortalece el control de las fronteras exteriores de la Unión mediante la prevención y la lucha contra el terrorismo, narcotráfico y otras formas graves de delincuencia internacional, que comprende. Se trata de un concepto que define muy bien la Política Criminal de la Unión con relación al terrorismo en el que prima el binomio libertad-seguridad.

Entre las amenazas y desafíos comunes que contempla esta Estrategia se encuentra el terrorismo. La Unión Europea entiende que el terrorismo aprovecha la era de la sociedad globalizada y tecnológica, y que estas dos ventajas técnicas facilitan a los terroristas el acceso a las comunicaciones de alta velocidad, la alta movilidad y las transacciones financieras instantáneas.

Según la UE, “su alcance global, sus consecuencias devastadoras, su capacidad de reclutamiento, así como la difusión de propaganda vía Internet y los diferentes medios mediante los que se financia, hacen del terrorismo una amenaza significativa y en constante evolución.”²⁷¹ En una respuesta contundente a estas amenazas, además de las medidas de carácter normativo, la Unión Europea ha comenzado en este mismo periodo a avanzar en materia de cooperación policial y judicial²⁷² mediante la intervención activa de Europol y otras agencias.²⁷³ Por ejemplo, inicia mecanismos basados en el reconocimiento mutuo de sentencias judiciales, y la “orden de detención europea y disposiciones sobre congelación de activos”²⁷⁴, y promueve el intercambio de información entre los Estados Miembros.²⁷⁵

Entre toda la normativa y la estrategia político-institucional enunciada relativa a la lucha contra el terrorismo elaborada por la Unión Europea, merecen especial atención la Decisión Marco 2002/475/JAI²⁷⁶ y la Decisión Marco 2008/919/JAI²⁷⁷ por el aporte legislativo y la búsqueda de armonización. A tenor de ello se brinda con detenimiento un mayor análisis.

1. Decisión Marco 2002/475/JAI

La Decisión Marco 2002/475/JAI de 13 de junio de 2002, sobre la lucha contra el terrorismo, armoniza la definición de delitos sobre el terrorismo en todos los Estados Miembros de la Unión Europea, mediante la introducción de una definición común recogida en el artículo 1. Por medio de esta Decisión Marco, se entenderá por terrorismo o acto terrorista en la Unión Europea, cualquier acto intencionado que pueda perjudicar gravemente a un país o a una Organización Internacional, tipificado como delito según el Derecho nacional, cometido con el fin de:

1. «Intimidar gravemente a una población,
2. obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo,
3. o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional, mediante:
 - a. atentados contra la vida de una persona que puedan tener resultado de muerte;

²⁷¹ *Ibidem*, p. 13.

²⁷² Este hecho ha permitido la supresión de controles en las fronteras interiores de la Unión Europea facilitando la libertad de movimiento de personas dentro del espacio Schengen.

²⁷³ Por ejemplo: Eurojust, para fomentar la coordinación e intensificar la eficacia de las autoridades judiciales; y la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), para la gestión de la cooperación operativa de las fronteras exteriores de la UE.

²⁷⁴ CONSEJO EUROPEO (2010), opus cit., p. 18.

²⁷⁵ Entre otras medidas, la Unión Europea aspira a la creación de una base de datos con tecnología biométrica y un registro de nombres de pasajeros europeo (PNR), respetando la reglamentación en materia de protección de datos personales.

²⁷⁶ Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (DO L 164 de 22.6.2002).

²⁷⁷ Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo (DO L 330 de 9.12.2008).

- b. atentados graves contra la integridad física de una persona;
- c. secuestro o toma de rehenes;
- d. destrucciones masivas en instalaciones gubernamentales o públicas, sistemas de transporte, infraestructuras, incluidos los sistemas informáticos, plataformas fijas emplazadas en la plataforma continental, lugares públicos o propiedades privadas, que puedan poner en peligro vidas humanas o producir un gran perjuicio económico;
- e. apoderamiento ilícito de aeronaves y de buques o de otros medios de transporte colectivo o de mercancías;
- f. fabricación, tenencia, adquisición, transporte, suministro o utilización de armas de fuego, explosivos, armas nucleares, biológicas y químicas e investigación y desarrollo de armas biológicas y químicas;
- g. liberación de sustancias peligrosas, o provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas;
- h. perturbación o irrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas;
- i. amenaza de ejercer cualesquiera de las conductas enumeradas en las letras a) a h).»²⁷⁸

En una búsqueda de mayor armonización en torno a las definiciones, la Decisión Marco 2002/475/JAI introduce también una definición de lo que se entiende por ‘grupo terrorista’. Dicha Decisión Marco establece que grupo terrorista es “toda organización estructurada de más de dos personas, establecida durante cierto periodo de tiempo, que actúa de manera concertada con el fin de cometer delitos de terrorismo” entendiéndose asimismo por ‘organización estructurada’ a una organización “no formada fortuitamente para la comisión inmediata de un delito y en la que no necesariamente se ha asignado a sus miembros funciones formalmente definidas ni hay continuidad en la condición de miembro o una estructura desarrollada.”²⁷⁹ Es decir, en la definición recogida se alude permanentemente a la existencia de la organización previo al acto delictivo y de forma sostenida en el tiempo, así también como a la jerarquización de sus miembros.

En materia procesal, la Decisión Marco 2002/475/JAI establece normas de competencia a fin de garantizar que los delitos de terrorismo sean perseguidos de manera eficaz²⁸⁰, y asimismo en cuanto a la protección, asistencia y resarcimiento de daño, incorpora medidas con relación a las víctimas de delitos de terrorismo.²⁸¹

2. Decisión Marco 2008/919/JAI

En respuesta a la creciente amenaza del uso de Internet con fines terroristas, en el año 2008 se modificó la Decisión Marco 2002/475/JAI para incluir específicamente disposiciones sobre la incitación pública a cometer actos de terrorismo, el reclutamiento para pertenecer a un grupo terrorista y el adiestramiento de terroristas por medio de Internet, dando lugar a la Decisión Marco 2008/919/JAI.

En las consideraciones preliminares de la Decisión Marco 2008/919/JAI se reconoce que la Decisión Marco 2002/475/JAI ha servido de base jurídica al haber establecido una definición

²⁷⁸ Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (DO L 164 de 22.6.2002), art. 1.

²⁷⁹ *Ibidem*, art. 2.

²⁸⁰ *Ibidem*, art. 9.

²⁸¹ *Ibidem*, art. 10.

de terrorismo y que también constituyó tempranamente un marco político europeo común antiterrorista, lo que ha permitido la persecución de los delitos de terrorismo. No obstante, asimismo determina que:

«La amenaza terrorista ha crecido y se ha desarrollado rápidamente durante estos últimos años, con cambios en el modus operandi de los terroristas y sus partidarios, incluida la sustitución de grupos estructurados y jerárquicos por grupúsculos semiautónomos ligados entre ellos con flexibilidad.²⁸² Tales grupúsculos forman redes internacionales y recurren cada vez más a las nuevas tecnologías, en especial Internet.»²⁸³

De esta forma, en materia criminal, Internet abrió paso no solo a una nueva forma de operar por parte del terrorismo, sino también a una conceptualización nueva del fenómeno. Según Cano Paños, es posible hablar de un ‘Viejo’ y un ‘Nuevo’ terrorismo, en donde el ‘Viejo terrorismo’ representa una “amenaza concreta, predecible, procedente de un enemigo más o menos localizable e individualizable”, y el ‘Nuevo terrorismo’ una “amenaza difusa, impredecible, procedente de un enemigo no localizable y muchos menos individualizable.”²⁸⁴

Por medio de la Decisión Marco 2008/919/JAI, las nuevas tecnologías de la información son jurídicamente reconocidas como un nuevo instrumento de promoción y acción del terrorismo. En las consideraciones preliminares de la propia DM se detalla claramente que:

«Internet se utiliza para inspirar y movilizar a las 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... [...] ... [En Internet] 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.»²⁸⁵

La determinación de costes y riesgos mínimos para los grupos terroristas o para el sujeto en el que recae concretamente la acción terrorista, está dada por el hecho de que el uso de las nuevas Tecnologías de la Información y Comunicación permite una gran amortización de la herramienta digital en cuanto no solo no resulta prohibitiva su adquisición, sino que también facilita el desarrollo de la actividad delictiva de forma sostenida en el tiempo sin nuevos costes o costes adicionales.

En cuanto a los riesgos es determinante el hecho de que Internet favorece el anonimato y dificulta la persecución del delito, así como la determinación de la autoría. Adicionalmente en la investigación de un ilícito en donde median las nuevas tecnologías pueden tener lugar otros inconvenientes, en este caso de índole procesal, que dificulte la persecución del crimen, tales como la delimitación de jurisdicción y competencia.

²⁸² Se establece en esta Decisión Marco, respecto de la anterior, un cambio en la definición de lo que se entiende por ‘grupo terrorista’

²⁸³ Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo (DO L 330 de 9.12.2008), Consideración previa N.º 3.

²⁸⁴ CANO PAÑOS, Miguel Ángel (2015): «El binomio Internet/Terrorismo islamista. De una amenaza virtual a un peligro real. Una visión desde la Criminología y el Derecho penal», *presentación de Power Point*, Doctorado en la Universidad de Granada.

²⁸⁵ Decisión Marco 2008/919/JAI del Consejo, opus cit., Consideraciones previas.

La Decisión Marco 2008/919/JAI²⁸⁶, además de la incorporación de Internet como un herramienta para la comisión del delito de terrorismo, resulta también novedosa porque introduce nuevos delitos como la difusión de propaganda terrorista, el adoctrinamiento y/o adiestramiento de terroristas.

Estas nuevas actividades que realiza el terrorismo y que esta DM contempla están recogidas en su artículo 3, y se encuentran definidas conceptualmente bajo las tipificaciones de “provocación a la comisión de un delito de terrorismo”, “captación de terroristas” y “adiestramiento de terroristas.” Dichos delitos implican una acción propagandística sobre terrorismo con la finalidad de incitación al terrorismo, el reclutamiento y la radicalización. Todas ellas entendidas como actos de provocación a la comisión de un delito de terrorismo.

A todo efecto, la Decisión Marco 2008/919/JAI entiende por provocación a la comisión de un delito de terrorismo, lo siguiente:

«La distribución o difusión pública, por cualquier medio, de mensajes destinados a inducir a la comisión de cualesquiera de los delitos enumerados en el artículo 1, apartado 1, letras a) a h), cuando dicha conducta, independientemente de que promueva o no directamente la comisión de delitos de terrorismo conlleve el riesgo de comisión de uno o algunos de dichos delitos.»²⁸⁷

Asimismo, en la misma Decisión Marco se entiende por captación de terroristas, la “petición a otra persona de que cometa cualesquiera de los delitos enumerados en el artículo 1, apartado 1, letras a) a h), o en el artículo 2, apartado 2.”

Finalmente, se entiende por adiestramiento de terroristas la acción de:

«Impartir instrucciones sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos, con el fin de cometer cualesquiera de los delitos enumerados en el artículo 1, apartado 1, letras a) a h), a sabiendas de que las enseñanzas impartidas se utilizarán para dichos fines.»²⁸⁸

En síntesis, podríamos concluir en que la Decisión Marco 2008/919/JAI es un instrumento normativo de la Unión Europea relevante en el sentido en que se ha erigido de forma temprana como un referente en la persecución de la propaganda terrorista en Internet, y en los delitos derivados de la difusión de esta propaganda en la red.

La DM 2008/919/JAI ha servido de base para posteriores instrumentos que de forma paulatina han ido exigiendo el cumplimiento de mayores desafíos por parte de la Política Criminal de la UE. Tal como ha mencionado en el año 2012 la ONU, se trata de una herramienta modelo que:

«[...] proporciona una base para perseguir la difusión de la propaganda terrorista y la transmisión de conocimientos para la fabricación de bombas a través de Internet, en la medida en que dicha difusión se haga intencionalmente y cumpla los requisitos de los delitos mencionados.»²⁸⁹

²⁸⁶ Sustituye al art 3 de la Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo.

²⁸⁷ Art. 3.

²⁸⁸ *Ibidem*.

²⁸⁹ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), *opus cit.*, p. 25.

3. Directiva (UE) 2017/541

La Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo del 15 de marzo de 2017 relativa a la lucha contra el terrorismo²⁹⁰ es un instrumento de la Unión que requiere ser mencionado en la lucha contra el terrorismo yihadista por el gran impacto que ha tenido en todos los EEMM de la Unión Europea.²⁹¹

La Directiva (UE) 2017/541 introduce nuevas medidas de carácter normativo y para ello establece de forma detallada en su Título III la tipificación de los delitos relacionados con actividades terroristas, y en su Título IV unas disposiciones generales relativas a los delitos de terrorismo. Ambos títulos recogen de forma exhaustiva todas las acciones terroristas que puede cometer un sujeto o un grupo terrorista y define con precisión qué entiende la Unión Europea por contenido terrorista. Tal exhaustividad está orientada a minimizar las diferencias entre los EEMM y a promover la armonización penal.²⁹²

Adicionalmente, la Directiva (UE) 2017/541 establece sanciones para las personas físicas (art. 16) y determina la responsabilidad de las personas jurídicas (art. 17), así como las sanciones aplicables a las mismas (art. 18). El artículo 19 insta a cada EEMM a adoptar las medidas necesarias para establecer la jurisdicción y el enjuiciamiento conforme a criterios comunes de acción a fin de establecer una cooperación lateral entre los Estados Miembros.

Con relación a los terceros Estados se promueve la cooperación a fin de poder eliminar los contenidos terroristas en línea que se encuentren alojados fuera de la Unión Europea, pero cuya existencia promueva un impacto negativo en la región. Al respecto, en las consideraciones preliminares de la Directiva se destaca que:

«Un medio eficaz de combatir el terrorismo en internet es eliminar en origen los contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo. Los Estados Miembros deben esforzarse al máximo por cooperar con terceros países al objeto de garantizar la eliminación de contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo desde los servidores ubicados en su territorio. No obstante, cuando no sea factible la eliminación de estos contenidos en origen, también pueden ponerse en marcha mecanismos que bloqueen el acceso a los mismos desde el territorio de la Unión. Las medidas adoptadas por los Estados Miembros con arreglo a la presente Directiva para eliminar los contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo o, cuando esto no sea posible, para bloquear el acceso a dichos contenidos, podrían basarse en una actuación pública de carácter legislativo, no legislativo o judicial. En ese sentido, la presente Directiva se entiende sin perjuicio de la acción voluntaria emprendida por la industria de internet para evitar un uso indebido de sus servicios, ni de cualquier apoyo a una acción de estas características por parte de los Estados Miembros, como, por ejemplo, detectar y advertir de los contenidos terroristas. Independientemente de la base o el método elegido, los Estados Miembros deben garantizar que se facilite un nivel adecuado de certidumbre y previsibilidad jurídica a los usuarios y los

²⁹⁰ Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la DM 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo.

²⁹¹ Cabe señalar que, en el caso particular de España, esta Directiva dio lugar a la modificar el artículo 575 del CP español. Se analizará este artículo en el Capítulo N.º 10.

²⁹² Dado que las directivas son un instrumento de la UE que deben de ser traspuestas a las legislaciones internas, y que en esta transposición se brinda cierto grado de discrecionalidad a los Estados, existe un riesgo de que la armonización penal en lo relativo al terrorismo, sea débil. Para corregir ese riesgo, la UE suele ser muy precisa y exhaustiva en sus definiciones y en los tipos penales que persigue.

proveedores de servicios, así como la posibilidad de recurso judicial con arreglo al Derecho nacional. Cualquiera de estas medidas debe tener en cuenta los derechos de los usuarios finales, y cumplir los procedimientos jurídicos y judiciales existentes y la Carta de los Derechos Fundamentales de la Unión Europea.»²⁹³

Resulta fundamental señalar que la Directiva (UE) 2017/541 sustituye a la DM 2002/475/JAI como piedra angular de la justicia penal de los países de la UE en la lucha contra el terrorismo, y modifica partes de la DM 2005/671/JAI relativa al intercambio de información y cooperación sobre estos delitos.²⁹⁴

4. Decisión (UE) 2018/890

En el ámbito de la cooperación policial y judicial, la Decisión 2018/890 de la Unión Europea para la prevención del terrorismo²⁹⁵ es un instrumento normativo de gran importancia porque facilita el intercambio de información entre los EEMM, y entre los EEMM y las agencias e instituciones de la UE, todo ello aspectos fundamentales de la lucha contra el terrorismo yihadista en Europa.

Este instrumento introduce también por vez primera la posibilidad de adoptar medidas preventivas en el ámbito de la radicalización yihadista. La forma en que lo hace es designando a Europol como contacto común para el intercambio de información que realizan los EEMM entre sí acerca de las personas que viajen al extranjero bajo la sospecha de que sus motivaciones de viaje poseen alguna finalidad vinculada al terrorismo yihadista.²⁹⁶

Si bien Europol ya se encargaba de facilitar el intercambio de información para delitos graves desde su creación en el año 2009²⁹⁷, este trabajo se realizaba a voluntad de las partes y no se encontraba sistematizado.²⁹⁸

En adición a esta falta de sistematización, la información compartida antes de la Decisión 2018/890 se integraba en un marco de acción general de delitos dentro de la UE, y no específicamente de delitos de terrorismo y/o terrorismo yihadista. Y por último, antes de la Decisión 2018/890 no se poseía un enfoque preventivo en esta materia, por lo que las actuaciones policiales o judiciales no se orientaban a la prevención de los delitos terroristas,

²⁹³ Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, opus cit., Consideración previa N.º 22.

²⁹⁴ Ibidem, art. 22.

²⁹⁵ Decisión (UE) 2018/890 relativa a la celebración, en nombre de la Unión Europea, del Protocolo Adicional al Convenio del Consejo de Europa para la prevención del terrorismo.

²⁹⁶ Cabe señalar que esta tipificación atiende a las acciones corrientes del terrorismo yihadista que promueve los viajes al extranjero de simpatizantes, gran parte de ellos ideologizados mediante Internet, con el objeto de recibir adiestramiento militar. La Sentencia de la Audiencia Nacional, Sala de lo Penal, Res. 25/2016 (AN Penal 28 sep. 2016) de España, es una excelente muestra de las labores de adoctrinamiento y planificación de viaje que realiza el yihadismo. “La sentencia considera probado la existencia de ‘una auténtica plataforma de envío de combatientes yihadistas’. Sus miembros formaban un grupo autodenominado brigada Al Andalus, localizado principalmente en la ciudad de Madrid, y desde principios de 2011 hasta su desarticulación, en junio de 2014, realizaron labores de captación, radicalización, adoctrinamiento y posterior envío de voluntarios yihadistas para llevar a cabo acciones operativas de naturaleza terrorista, ‘integrados en las franquicias de Al Qaeda’”. Disponible en: <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/La-Audiencia-Nacional-condena-a-la-celula-yihadista-liderada-por-Lahcen-Ikassrien> [Fecha de consulta: 21 de noviembre de 2023].

²⁹⁷ Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (EUROPOL).

²⁹⁸ Eso significa que antes de la Decisión (UE) 2018/890, los EEMM compartían información entre sí de forma espontánea y voluntaria. No existía una institucionalización de la cooperación policial y judicial, y por lo tanto de se carecía de sistematización en este sentido. Ello dejaba un amplio margen discrecional a cada Estado Miembro acerca de cómo compartir información, y acerca de qué información compartir.

sino a la persecución de los actos terroristas ya cometidos. La singularidad más destacada, por tanto, de la Decisión 2018/890 de la Unión Europea, es su especificidad en cuanto al intercambio de información a fin de prevenir los actos de terrorismo. Es decir, la posibilidad de actuar colaborativamente, pero primordialmente de forma temprana entre todos los EEMM de la Unión.

Respecto a la tipificación en esta orientación preventiva, considera una serie de actos recogidos entre el artículo 2 y el artículo 6, entre los cuales se incluyen la participación en grupos o asociaciones con fines de terrorismo (artículo 2); el adiestramiento con fines de terrorismo (art. 3); los viajes al extranjero con fines de terrorismo (artículo 4); la financiación de los viajes al extranjero con fines de terrorismo (artículo 5); y, la organización o cualquier otra forma de facilitación de los viajes al extranjero con fines de terrorismo (artículo 6). La amplia tipificación de la Decisión (UE) 2018/890 convierte a esta Decisión en un instrumento de vital importancia en la prevención del terrorismo yihadista al facilitar el marco legal adecuado para la cooperación lateral entre los EEMM mediante la actuación directa y preventiva de Europol.

DERECHO DEL CONSEJO DE EUROPA REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS

En el año 2001, el Consejo de Europa desarrolló el Convenio de Budapest.²⁹⁹ Dicho Convenio, también conocido como el Convenio sobre Ciberdelincuencia, tiene por objeto armonizar las legislaciones nacionales de la UE relativas al delito cibernético³⁰⁰. El Convenio sobre Ciberdelincuencia³⁰¹ se ha constituido como el primer acuerdo comunitario que busca hacer frente a los delitos informáticos y los delitos realizados mediante el uso de Internet por medio de la armonización de las legislaciones internas de los EEMM y a través del incremento de la cooperación policial y judicial de las partes firmantes.

Representa, por tanto, un instrumento regional jurídicamente vinculante que aborda la actividad delictiva en Internet. “El convenio establece una norma mínima común respecto de los delitos internos cometidos con computadoras”,³⁰² entre ellos: el acceso no autorizado a sistemas, fraude y falsificación informática, manipulación ilícita de programas, abuso sexual infantil, propiedad intelectual, etc.

El Convenio contiene también disposiciones en materia procesal para facilitar la obtención de pruebas de actos de terrorismo cometidos por Internet. No obstante, estos procedimientos deben estar sujetos a las garantías aplicables establecidas en las legislaciones nacionales de cada Estado parte de la Unión. Por ejemplo, el Convenio sobre la Ciberdelincuencia del Consejo de Europa obliga a las partes a la promulgación de leyes internas que permitan exigir a los

²⁹⁹ CONSEJO DE EUROPA (2001): *Convenio sobre la Ciberdelincuencia*, Serie de Tratados N.º 185, de 23 de noviembre de 2001.

³⁰⁰ En el preámbulo del Convenio se enuncia: “[...] la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la Ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional [...]”

³⁰¹ Elaborado por el Consejo de Europa en Estrasburgo, con la participación de Canadá, Japón y China como terceros Estados observadores.

³⁰² Informe explicativo del Convenio sobre la Ciberdelincuencia del Consejo de Europa, párr. 33. Véase: UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 22.

proveedores de Internet la conservación de los datos almacenados en sus servidores por un periodo máximo de 90 días (renovables), para el caso de que sea requerida dicha información y se deba hacer cumplir esta ley, en el curso de una investigación o procedimiento penal.³⁰³

Este procedimiento es de suma importancia considerando la naturaleza efímera de los datos electrónicos. La emisión de una orden de conservación o una medida cautelar similar también tiene varias ventajas en comparación con los procedimientos tradicionales de registro e incautación, ya que el proveedor de servicios de Internet puede estar en mejores condiciones de obtener rápidamente las pruebas necesarias. En adición, y respecto a la protección de la prueba, el artículo 19 del Convenio sobre la Ciberdelincuencia, “confiere a los datos almacenados una protección similar a que suelen otorgarse a las pruebas tangibles de acuerdo con la legislación nacional pertinente”.

En una búsqueda de máxima armonización para todos los Estados Miembros en relación con el procedimiento, el Convenio obliga a las partes involucradas a presentar los datos de los abonados a fin de identificar al abonado al servicio de Internet.³⁰⁴

Esta información del abonado puede resultar vital en la etapa de la investigación a fin de determinar la identidad del autor del acto terrorista en el cual se haya involucrado algún tipo de usabilidad de Internet.

El Convenio sobre la Ciberdelincuencia adicionalmente contempla, entre sus medidas de cooperación regional para la prevención del terrorismo y para la actuación en las investigaciones, aspectos tales como el suministro de información no solicitada.³⁰⁵

El artículo 26 del Convenio sobre la Ciberdelincuencia se refiere específicamente a la información espontánea, sin que exista demanda previa, y con relación a ella se especifica que:

«[...] una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el propio Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte [...]»³⁰⁶

Merece especial atención el Protocolo adicional al Convenio sobre la Ciberdelincuencia³⁰⁷ relativo a los delitos de índole racista y xenófobo por medio de sistemas informáticos, en atención al hecho de que facilita “el enjuiciamiento de los actos de terrorismo cometidos por Internet con la intención de incitar a la violencia por motivos de raza, color, ascendencia u origen nacional o étnico, o religión.”³⁰⁸

Conforme a la descrito en el Protocolo adicional del Convenio sobre la Ciberdelincuencia, se insta a cada Parte a la adopción de medidas legislativas en su derecho interno, siempre que tenga lugar, de forma intencional, la siguiente conducta:

³⁰³ *Ibidem*; p. 23.

³⁰⁴ CONSEJO DE EUROPA (2001), opus cit., artículo 18.

³⁰⁵ “El [...] Convenio prevé el intercambio con otras partes de información no solicitada en relación con investigaciones o actuaciones, dentro de los límites impuestos por la legislación nacional, en el interés común de responder a los actos delictivos (información espontánea).” Véase: UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 24.

³⁰⁶ CONSEJO DE EUROPA (2001), opus cit., artículo 26.1.

³⁰⁷ CONSEJO DE EUROPA (2003): *Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*, Serie de Tratados N.º 189, de 28 de enero de 2003.

³⁰⁸ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 25.

«[...] amenazar, por medio de un sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o, ii) a un grupo de personas que se distinga por alguna de esas características.»³⁰⁹

En el propio Protocolo adicional, en su artículo 5, se recoge expresamente la disposición de que cada parte debe adoptar las medidas legislativas necesarias a fin de tipificar como delito tales conductas en sus derechos internos.³¹⁰

En el marco de la legislación del Consejo de Europa referente a la lucha contra el terrorismo, además del citado Convenio sobre la Ciberdelincuencia, es necesario mencionar un documento previo que ha servido de herramienta temprana para el desarrollo normativo posterior del Consejo de Europa. Este es el Convenio Europeo de Estrasburgo para la Represión del Terrorismo del 27 de enero de 1977.³¹¹ El Convenio Europeo de Estrasburgo para la Represión del Terrorismo, en su artículo 1 enumera los actos ilícitos que se consideran delitos de terrorismo, tales como la captura ilícita de aeronaves, ataques contra la vida y la integridad corporal o la libertad de las personas con derecho a protección internacional, delitos que impliquen raptos, toma de rehenes o secuestro, etc.

Naturalmente, por la fecha en la que el instrumento fue elaborado (1977), no existen descripciones dentro de esta normativa acerca de las nuevas formas del terrorismo, y debido a ello al presente podría considerarse un documento en apariencia básico en la lucha contra esta forma criminal. No obstante, este Convenio ha supuesto las bases tempranas para dos elementos coyunturales y relativos a la definición y prevención.

En primer lugar, debemos de partir de la idea de que el principal objetivo del Convenio Europeo de Estrasburgo para la Represión del Terrorismo era establecer que “los delitos terroristas no pueden considerarse delitos políticos, ni delitos relacionados con los delitos políticos, ni delitos inspirados por motivos políticos.”³¹² Ello es altamente relevante debido al problema de definición conceptual al que hacíamos referencia al inicio de este estudio. El Convenio Europeo de Estrasburgo para la Represión del Terrorismo busca sentar de este modo las bases tempranas para delimitar el problema y evitar la disgregación del concepto de terrorismo, al establecer

³⁰⁹ CONSEJO DE EUROPA (2003), opus. cit., art. 4. En el art. 4 del Protocolo adicional al Convenio sobre la Ciberdelincuencia. Legislar sobre este hecho posee especial relevancia y carácter preventivo porque, aun cuando no se refiere está normativa a delitos cuyas acciones terroristas directas deriven en un atentado, dichas acciones de racismo y xenofobia sí que acrecientan el marco ideológico de odio que promueve los posteriores actos terroristas del yihadismo. Véase: TORRENS, Xavier (2023): «El islamismo radical se caracteriza por su racismo anti-occidental/ Entrevistado por I. Ellakuría», *Periódico El Mundo*, edición online de 29 de enero de 2023. Disponible en: <https://www.elmundo.es/espana/2023/01/29/63d53b27e4d4d89f7c8b456e.html> [Fecha de consulta: 21 de noviembre de 2023]. Véase: BOUREKBA, Moussa (2020): «La extrema derecha violenta y el yihadismo comparten una misma cosmovisión/ Entrevistado por P. Simón», *Revista La Marea*, edición online de 3 de julio de 2020. Disponible en <https://www.lamarea.com/2020/07/03/extrema-derecha-violenta-y-yihadismo-comparten-cosmovision/> [Fecha de consulta: 21 de noviembre de 2023].

³¹⁰ España lo ha hecho con una normativa específica relativa a Delitos de odio en Internet.

³¹¹ CONSEJO DE EUROPA (1977): *Convenio Europeo de Estrasburgo para la represión del terrorismo*, Serie de Tratados N.º 090, de 27 de enero de 1977.

³¹² [20] (2), Propuesta de Decisión Marco del Consejo sobre la lucha contra el terrorismo, COM/2001/0521 final, CNS 2001/0217 Diario Oficial N.º 332 E de 27/11/2001, p. 0300-0304. 52001PC0521. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A52001PC0521#:~:text=El%20Convenio%20Europeo%20para%20la%20Represión%20de%20Terrorismo%20%5B21%5D%2C,delitos%20inspirados%20por%20motivos%20pol%C3%ADticos>. [Fecha de consulta: 21 de noviembre de 2023].

claramente que los delitos terroristas suponen una categorización diferente (más grave) que los delitos políticos.

En segundo lugar, en una clara y anticipada referencia sobre la prevención de los actos terroristas el Convenio Europeo de Estrasburgo para la Represión del Terrorismo (1977) extiende su protección por medio del artículo 1 inciso f, mediante el cual se penaliza “la tentativa de comisión de alguno de los delitos anteriormente mencionados o la participación como coautor o cómplice de una persona que cometa o intente cometer dichos delitos”.³¹³

En referencia a la tentativa de comisión del delito la normativa se refiere a la fase necesaria de planeación y de instrucción para la comisión de un atentado terrorista.

En la actualidad está claro que estas fases pueden ser llevadas a cabo a través de Internet mediante el intercambio de comunicaciones secretas en la red. Sin embargo, en la fecha de elaboración de este instrumento normativo naturalmente no se pensaba en términos digitales debido a su inexistencia, por ello lo relevante de este artículo 1 inciso f radica en el hecho de ampliar la protección a un ámbito de tentativa. La regulación normativa que propone el Convenio Europeo de Estrasburgo en este aspecto hace suponer una temprana inclinación de la Política Criminal de Europa hacia el modelo preventivo.

Así como el Protocolo Adicional del Convenio sobre Ciberdelincuencia se centra en los delitos de racismo y xenofobia como antesala ideológica a la comisión de un atentado yihadista, el Convenio Europeo de Estrasburgo para la Represión del Terrorismo establece su atención en los actos preparatorios del delito en Internet. Ambos instrumentos normativos adquieren por tanto una orientación preventiva que faculta tempranamente a las actuaciones policiales y judiciales de nuestro presente.

Ante el incremento de la amenaza terrorista en Europa se aprueba el Convenio del Consejo de Europa para la Prevención del Terrorismo³¹⁴ (Varsovia, 2005), cuya intención principal es el establecimiento de una relación más estrecha entre los Estados Miembros de la Unión Europea, reconociendo la necesidad de intensificar la cooperación en esta materia entre todas las Partes. Este Convenio posee una clara connotación preventiva respecto al terrorismo.

El artículo 3 es especialmente relevante y configurador de la Política Criminal de la Unión en esta materia, debido a que se orienta a reforzar jurídicamente las otras dos medidas de la Política Criminal que analizaremos en los siguientes capítulos

El artículo 3, inciso 2 del Convenio del Consejo de Europa para la Prevención del Terrorismo detalla que:

«Cada Parte tomará las medidas necesarias para mejorar y desarrollar la cooperación entre las autoridades nacionales con vistas a prevenir los delitos terroristas y sus efectos negativos, en particular mediante:

³¹³ Es pertinente señalar que esta extensión de protección del Convenio Europeo de Estrasburgo supone una tempranísima orientación *ad hoc* a las nuevas formas de terrorismo que introduce el surgimiento de Internet. Cabe recordar que dicho Convenio es un instrumento que data de 1977, año en el que Internet aún se encontraba restringido a los ámbitos gubernamentales y académicos, y por tanto aún no existía el desarrollo global y democrático de la red en los mismos términos de usabilidad que hoy se conoce.

³¹⁴ CONSEJO DE EUROPA (2005): Convenio del Consejo de Europa para la prevención del terrorismo, Varsovia, 16 de mayo de 2005.

- a) El intercambio de información;
- b) el refuerzo de la protección física de las personas y de los bienes;
- c) la mejora de los planes de formación y coordinación para situaciones de crisis.»

Estas actuaciones descritas en el artículo 3.2 del Convenio insta a todos los Estados Miembros de la Unión a la adopción de medidas eficaces e institucionalizadas de forma permanente para prevenir el terrorismo y para hacer frente a los crímenes terroristas, con especial atención a los cometidos mediante sistemas de cómputo. Se apoya también en el artículo 4 para promover la asistencia y el apoyo mutuo entre EEMM para el cumplimiento de estos fines.

El artículo 3 promueve también un aspecto de carácter preventivo (que desarrollaremos en el Capítulo 7 de esta investigación), por cuanto se centra en el fomento de campañas de información y concienciación de la población europea. El artículo 3 del Convenio para la Prevención del Terrorismo, adquiere debido a ello una nueva dimensión al abordar una temática no considerada hasta entonces en instrumentos normativos europeos previos: la creación de contra discursos. El artículo 3, inciso 1, 3 y 4 promueve el desarrollo de medidas de sensibilización de la población a fin informar, generar conciencia del terrorismo y los riesgos en torno a la captación, a promover la tolerancia y a ser un ciudadano europeo activo y comprometido con la prevención del terrorismo dentro del territorio de la Unión. Textualmente establece que:

«1. Cada Parte tomará las medidas apropiadas, en particular en el ámbito de la formación de las autoridades encargadas del cumplimiento de la ley y otros órganos, así como en el ámbito de la educación, la cultura, la información, los medios de comunicación y la sensibilización del público, con vistas a prevenir los delitos terroristas y sus efectos negativos, respetando al propio tiempo las obligaciones relativas a los derechos humanos que le incumban, tal como se establecen en el Convenio para la protección de los derechos humanos y de las libertades fundamentales, en el Pacto Internacional de derechos civiles y políticos, y otras obligaciones relativas al derecho internacional, cuando le sean aplicables.

3. Cada Parte promoverá la tolerancia fomentando el diálogo interreligioso y transcultural, fomentando, en su caso, la participación de organizaciones no gubernamentales y otros actores de la sociedad civil, con objeto de prevenir tensiones que podrían contribuir a la comisión de delitos terroristas.

4. Cada Parte se esforzará por sensibilizar mejor al público sobre la existencia, las causas, la gravedad y la amenaza que suponen los delitos terroristas y los delitos previstos en el presente Convenio, y considerará la posibilidad de alentar al público a prestar a las autoridades competentes una ayuda concreta y específica que pueda contribuir a la prevención de delitos terroristas y de los delitos previstos por el presente Convenio.»

Este enfoque orientado a las campañas preventivas resulta altamente novedoso y adecuado a los tiempos modernos. Internet ha facilitado las acciones delictivas del yihadismo, pero también es una herramienta que permite la difusión activa de diversos actores de la sociedad de campañas en el fomento del diálogo, la prevención y la acción ciudadana. El artículo 3, inciso 1, 3 y 4 del Convenio para la Prevención del Terrorismo faculta entonces al desarrollo de medidas preventivas, no solo de carácter policial y judicial, sino también en torno a la noción ideológica y discursiva del problema de terrorismo. Este hecho es un gran acierto en cuanto permite un amplio desarrollo de la tercera medida (medidas preventivas y campañas de información y concienciación en la población europea) de la Política Criminal de Europea con relación al terrorismo yihadista.

El Convenio sobre la Ciberdelincuencia (Budapest, 2001) y el Convenio para la Prevención del Terrorismo (Varsovia, 2005), ambos elaborados por el Consejo de Europa, son dos instrumentos que pueden aplicarse de forma conjunta con la finalidad de brindar más protección en lo referente al uso de Internet con fines terroristas. Cabe señalar que algunas de las disposiciones y directrices de ambos Convenios han sido utilizadas de forma literal por los Estados Miembros en la elaboración de sus legislaciones nacionales orientadas a reprimir y a concienciar sobre el yihadismo online, así como sobre el cibercrimen.

El Convenio del Consejo de Europa para la Prevención del Terrorismo permite triangular con Europol la prevención del terrorismo con los EEMM, y también entre EEMM y agencias e instituciones de la Unión. A su vez, el Convenio facilita la cooperación horizontal entre los EEMM entre sí. Esto último se implementa mediante el reconocimiento mutuo de sentencias, y la orden de detención europea, mientras que a su vez promueve la información espontánea para el fortalecimiento del Espacio de libertad, seguridad y justicia (ELSJ).

Se suma también a este esfuerzo normativo, en el año 2015, el Protocolo adicional al Convenio del Consejo de Europa para la prevención del terrorismo.³¹⁵ Este Protocolo facilita la cooperación para establecer una red de puntos de contacto nacionales activos 24x7 para facilitar el rápido intercambio de información.

Resulta aplicable también a este modelo orientado a la prevención, aunque no pertenece al Consejo Europeo, la previamente citada Decisión 2018/890 de la Unión Europea para la prevención del terrorismo. La Decisión (UE) 2018/890 designa en este caso a Europol como contacto común para el intercambio de información acerca de las personas que viajan al extranjero³¹⁶ para recibir adiestramiento militar y posteriormente regresar a Europea con fines de realizar la yihad³¹⁷ en territorio comunitario.

Todas estas medidas son normativa aplicable europea y se orientan a reforzar la lucha contra el terrorismo yihadista en la región, y brindar un marco jurídico a la cooperación institucional y a la prevención, otros dos elementos fundamentales en la Política Criminal de la Unión Europea.

LA INFLUENCIA DEL DERECHO INTERNACIONAL REFERENTE A LA LUCHA CONTRA EL USO DE INTERNET CON FINES TERRORISTAS

El marco jurídico internacional referente a la lucha del uso de Internet con fines terroristas comprende una gran variedad de fuentes, entre ellas, las resoluciones de las Naciones Unidas³¹⁸, los instrumentos jurídicos universales, los acuerdos regionales³¹⁹ y las leyes modelo.

³¹⁵ CONSEJO DE EUROPA (2015): *Protocolo adicional al Convenio del Consejo de Europa para la prevención del terrorismo*, Riga, 22 de octubre de 2015, (DOUE de 22 de junio de 2018).

³¹⁶ Se refiere a las fronteras exteriores de la Unión Europea, y concretamente a los territorios de instrucción yihadista donde existen campos de entrenamiento, principalmente Siria e Irak.

³¹⁷ La palabra *yihad* se utiliza habitualmente para definir la ‘guerra santa’ que realizan los terroristas yihadistas contra Occidente. La palabra *yihad* posee otras connotaciones (religiosas y etimológicas) que carecen de importancia en este contexto.

³¹⁸ Las resoluciones de las Naciones Unidas resultan sumamente relevantes. Por ejemplo, “*Las resoluciones del Consejo de Seguridad pueden imponer obligaciones jurídicamente vinculantes para los Estados Miembros o proporcionar fuentes de compromisos políticos de derecho incipiente*” en UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 17.

³¹⁹ Las obligaciones emanadas de los tratados celebrados solo son vinculantes para aquellos Estados que deciden ser parte en los acuerdos.

El protagonismo de las Naciones Unidas en esta lucha ha sido siempre indiscutible. Este organismo se ha pronunciado en múltiples resoluciones respecto a la lucha contra el terrorismo internacional, propiciando y fomentando de esta forma las iniciativas multilaterales dentro del Sistema internacional.

En el desarrollo y sostenimiento de esta cooperación entre todos los Estados Miembros, el 8 de septiembre de 2006 la Asamblea General aprobó la Estrategia global de las Naciones Unidas contra el terrorismo mediante la publicación de la Resolución 60/288. Conforme al plan de acción de este documento, se propuso como punto inicial:

«[...] condenar de manera sistemática, inequívoca y firme el terrorismo en todas sus formas y manifestaciones, independientemente de quien lo cometa y de donde y con que propósitos, puesto que constituye una de las amenazas más graves para la paz y seguridad internacional.»³²⁰

En esta Resolución se enumera, entre otras acciones, la voluntad de adoptar medidas urgentes para prevenir y combatir el terrorismo ajustándose a las obligaciones derivadas del Derecho internacional, considerando en ello, la Carta de las Naciones Unidas, las normas de derechos humanos, el derecho de los refugiados y el derecho internacional humanitario. Es decir, las Naciones Unidas (al igual que la Unión Europea) se inclina hacia la propuesta de soluciones activas y contundentes de erradicación del crimen de terrorismo, considerando siempre la salvaguarda que brindan los valores constitucionales de un Estado democrático. Tal como expresa Ana Pérez Machío, “la defensa de los derechos humanos y el mantenimiento del imperio de la ley en la lucha contra el terrorismo es el elemento central de las recomendaciones del Secretario General para una estrategia mundial contra el terrorismo.”³²¹

La Resolución 60/288 propone paralelamente medidas para hacer frente a las condiciones que favorecen o propician la propagación del terrorismo, tales como los conflictos prolongados sin resolver, la discriminación por motivos étnicos, nacionales o religiosos, exclusión político-económica. No obstante, es determinante al expresar que estas condiciones no pueden ser nunca justificación de actos de terrorismo. En el punto 2 de la Resolución, denominado *Medidas para prevenir y combatir el terrorismo*, se hace hincapié en la necesidad de establecer una férrea cooperación internacional en la lucha contra el terrorismo, facilitando el intercambio de información, cooperando en investigación, fortaleciendo el imperio de la ley y adoptando medidas de investigación adecuadas antes de la concesión de asilo.³²²

Como máxima expresión de cooperación internacional en esta materia se ha planteado plausible el establecimiento de un centro internacional de lucha contra el terrorismo, dando paso de esta forma al establecimiento de la cooperación internacional institucionalizada.³²³ En consonancia con esta propuesta de estrategia multilateral se invita, en el marco de esta resolución, al sistema

³²⁰ UN. A/RES/60/288; p. 3.

³²¹ PÉREZ MACHÍO, Ana I. (2008): «Normativa internacional para la erradicación de todas las formas de terrorismo», en: DE LA CUESTA, José Luis/MUÑAGORRI, Ignacio (Dir.), *Aplicación de la normativa antiterrorista*, Donostia: IVAC/KREI, p. 27.

³²² Busca establecer por medio de la investigación exhaustiva de los solicitantes una mayor protección en el ámbito de la concesión dentro del derecho de asilo, debido a que ha sido un recurso muy utilizado por miembros del yihadismo para ingresar a Europa o a Estados Unidos con la secreta finalidad de cometer atentados una vez obtenido dicho derecho.

³²³ “Reconocer que podría estudiarse la cuestión de establecer un centro internacional de lucha contra el terrorismo, como parte de los esfuerzos internacionales para intensificar la lucha contra el terrorismo.” *Ibidem*; p.6.

de las Naciones Unidas y los Estados Miembros a la elaboración de una base de datos internacional única que comprenda incidentes de terrorismo biológico a fin de completar la base de datos sobre delitos biológicos prevista por la Organización Internacional de la Policía Criminal (INTERPOL).³²⁴

Adicionalmente a la Resolución 60/288, en los últimos años el Consejo de Seguridad ha aprobado una serie de resoluciones bajo la premisa de potenciar la lucha contra el terrorismo y la de obligar a los Estados Miembros a colaborar sin reservas en la cooperación con otros gobiernos.

Así, por ejemplo, “las resoluciones 1373 (2001) y 1566 (2004) requieren que todos los Estados Miembros adopten medidas legislativas y de otro tipo para luchar contra el terrorismo”³²⁵ en materia de investigación, detención, extradición y enjuiciamiento de personas involucradas en actos terroristas.

En cuanto al uso de Internet con propósitos terroristas debe de tenerse en cuenta especialmente la Resolución 1624 (2005) en la cual el Consejo de Seguridad ha abordado la necesidad de la persecución penal de los delitos de incitación y glorificación (apología) de los actos de terrorismo. Si bien esta resolución no se refiere exclusivamente al hecho de que estos dos delitos se cometan utilizando exclusivamente medios informáticos, sí que debemos tener en cuenta que son dos delitos que el yihadismo realiza de forma profusa y sostenida mediante el uso de Internet. Es decir, la aparición y desarrollo de Internet ha propiciado el incremento sin precedentes de estos dos delitos mencionados, de ahí que sea necesario destacar la importancia de esta resolución en el ámbito del terrorismo en la red.

En los últimos informes y resoluciones de las Naciones Unidas se incorpora a Internet como a un elemento de vital importancia en la lucha contra el terrorismo. Y ello lo hace en dos vertientes: uno, utilizando Internet como un instrumento de lucha contra el terrorismo³²⁶; y dos, reconociendo la importancia del uso de Internet con fines terroristas en la amplia estrategia de lucha contra el terrorismo.

En el año 2006, en un informe de la Asamblea General denominado *Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo*³²⁷ se hace referencia al uso de Internet con fines terroristas. En el punto C del informe, en su inciso 58 y 59 (*Negar el acceso a la comunicación y al proselitismo luchando contra el uso de Internet por los terroristas*) se detalla que en vista de que las redes terroristas dependen de la comunicación para el reclutamiento de nuevos miembros, lo prioritario sería impedirles la utilización de Internet, para poder evitar de este modo la utilización de este medio como un vehículo delictivo, especialmente para el delito de propaganda.

En dicho informe se establece que el uso propagandístico de Internet ha facilitado en la última década se haya desarrollado un crecimiento acelerado de sitios yihadistas online. De hecho, el informe cuantifica este crecimiento citando el hecho de que en el año 1998 los terroristas tenían menos de 20 sitios web disponibles en la red, siendo para fines del año 2005 aproximadamente

³²⁴ Se alienta también en este aspecto a la creación de listas de expertos, de laboratorios y de procedimientos técnicos.

³²⁵ UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 18.

³²⁶ En la Resolución 60/288, concretamente en su punto 12, inciso b, enuncia que se debe: “utilizar Internet como instrumento para luchar contra la propagación del terrorismo, reconociendo al mismo tiempo que los Estados pueden necesitar asistencia a este respecto”

³²⁷ UN. A/60/825.

un millón de sitios web activos con información de combate y propaganda yihadista. En efecto, en el propio informe se reconoce que “algunos de los principales atentados recientes se apoyaron en información obtenida de Internet.”; y que “Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional.” Con relación a esta transaccionalidad, en el informe *Unidos contra el terrorismo* se reconoce que la propia naturaleza de Internet permite que aquellas personas que quieran utilizar la red con fines terroristas pueden hacerlo desde cualquier parte del mundo.

En el mismo orden de análisis, en el año 2010 el Consejo de Seguridad, mediante la Resolución 1963, enunció:

«[...] su preocupación ante la creciente utilización por los terroristas, en una sociedad globalizada, de nuevas tecnologías de la información y las comunicaciones, en particular Internet, con fines de reclutamiento e incitación, así como para financiar, planificar y preparar sus actividades.»

Como es notorio, ante el incremento exponencial de sitios terroristas en Internet y ante la adhesión al yihadismo de cada vez un mayor número de personas captadas por medio de la red, el Consejo de Seguridad, y los Estados Miembros de la ONU, han centrado sus esfuerzos en la vigilancia y en la prevención del terrorismo en Internet.

Debe destacarse no obstante que, si bien existe un número considerable de resoluciones aprobadas en el seno de las Naciones Unidas orientadas a la lucha contra el terrorismo, y aun cuando el número de adhesiones a esos instrumentos ha aumentado en los últimos años, actualmente no existe ningún tratado global de las Naciones Unidas contra el terrorismo que sea aplicable a todas las formas y manifestaciones de terrorismo.³²⁸

Si bien desde el año 2000 se tiene la pretensión de elaborar un convenio general, ante la dificultad de alcanzar un consenso se ha ido trabajando paulatinamente en instrumentos de forma sectorial orientados a las diferentes manifestaciones del terrorismo.³²⁹ Estos instrumentos son los que sirven de base para combatir al presente el uso de Internet con fines terroristas, dado que hasta el momento no existe ningún convenio universal que trate específicamente esta materia.

Aun así, en el marco de las Naciones Unidas, se aprobó, en diciembre de 2010, la resolución 65/230. La Resolución 65/230 tomó en consideración la *Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución* y solicitó a la Comisión de Prevención del Delito y Justicia Penal que estableciera, con arreglo a lo dispuesto en la Declaración de Salvador, un grupo intergubernamental de expertos de composición abierta. Este grupo intergubernamental de expertos se propuso para que realizara un estudio exhaustivo del problema del delito cibernético y de las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante este fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional.³³⁰

³²⁸ Principalmente porque no existe una definición internacional jurídicamente vinculante del término.

³²⁹ [Los] “instrumentos se centran en la penalización de determinados ‘actos terroristas’, sin definir el concepto más amplio de terrorismo”. Véase: UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 20.

³³⁰ *Ibidem*; p. 21.

Se espera que los resultados de este estudio, que se inició en el año 2012, faciliten la evaluación de los efectos del uso de las nuevas tecnologías de la información en actividades criminales, en particular información referida a los usos terroristas de Internet, tales como el delito de incitación al terrorismo y a la comisión de delitos de financiación del terrorismo por medios electrónicos.

Sí bien la cooperación en el ámbito internacional en cuanto a la lucha contra el terrorismo es mucha, se debe de tener en cuenta que los instrumentos universales de los que se dispone hasta el momento no definen los delitos terroristas como delitos con arreglo al derecho internacional. En vista de ello, se obliga a los Estados parte a tipificar en sus derechos internos las conductas ilícitas y sus respectivas penas, a determinar la competencia respecto de los autores, y a establecer mecanismos de cooperación internacional en lo referente a enjuiciamiento y en materia de extradición. Ello significa que en el marco internacional la persecución del terrorismo y/o yihadismo global en Internet está más orientada a la cooperación entre Estados que a la lucha con instrumentos comunes.

Es fundamental concluir en que mientras no se disponga de un instrumento de uso global, “los acuerdos bilaterales y multilaterales deberán servir de base para la elaboración de normas comunes para combatir el uso de Internet con fines terroristas, en aras de la promoción de la cooperación internacional.”³³¹

³³¹ *Ibidem*.

CAPÍTULO 6: MEDIDAS INSTITUCIONALES DE LA UNIÓN EUROPEA TENDIENTES A LA COOPERACIÓN EN EL CONTROL Y VIGILANCIA DE INTERNET Y A LA REPRESIÓN SOBRE SU USO CON FINES YIHADISTAS

LA COOPERACIÓN EUROPEA INSTITUCIONALIZADA REFERENTE AL USO DE INTERNET CON FINES YIHADISTAS

La cooperación europea institucionalizada comienza a tener solidez a partir del Tratado de Lisboa de 2007. El Tratado de Lisboa es el instrumento jurídico que, en el marco de la cooperación en seguridad, ha permitido la creación del Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI). El desarrollo principal de este Comité es la evaluación de amenazas y prioridades tanto nacionales, como de la Unión Europea. Entre las diferentes evaluaciones que realiza este Comité y otras agencias de la Unión Europea, destaca el trabajo estratégico para el fomento del desarrollo de nuevas tecnologías desde un enfoque común a fin de acrecentar la eficiencia en la instrumentalización de programas de vigilancia en Internet. De igual forma, busca “incrementar la relación entre el sector público y privado, incentivando los programas de investigación y desarrollo en materia de seguridad.”³³²

La Política Criminal actual de la UE referente a la lucha contra el terrorismo en Internet se basa en poseer un rol de liderazgo en el Sistema internacional, con arreglo al respeto de los Derechos Humanos. La Estrategia de la Unión Europea de Lucha contra el Terrorismo del 2005, sentó la base fundacional de la Política Criminal de la Unión en esta materia, y permitió establecer el marco de actuación de cooperación institucional. Este compromiso se materializó luego de los ataques terroristas de Madrid (11/3/2004) y Londres (7/7/2005). Desde entonces, la adopción de una estrategia común, que posteriormente se fue revisando y actualizando, ha permitido a la UE llevar a cabo acciones de forma coordinada.

Si bien el punto de inflexión en la prevención y lucha contra el terrorismo dentro de la Unión Europea y el propio Sistema internacional, se produce como consecuencia a los atentados del 11 de septiembre, son los ataques terroristas de Madrid y Londres aquellos que resultan determinantes para la adopción de medidas comunes dentro de la Unión. Al respecto, Carmela Pérez Bernárdez, reseña que:

«El hecho de que el Consejo Europeo identificara al terrorismo como un reto global, una vez perpetrados los atentados del 11 de septiembre y convirtiera la lucha contra el mismo, más que nunca, en un objetivo prioritario de la UE, constituye la primera piedra de una estrategia global en la materia.

En Naciones Unidas, el mismo mes en que se produjeron los atentados de Madrid de 2004, se revitaliza el Comité contra el Terrorismo, estableciendo una Dirección Ejecutiva que asistiría al desempeño de sus tareas. También en la UE, tras el 11 de septiembre, de nuevo, una vez que tuvo lugar este primer gran atentado terrorista internacional en el territorio de un Estado Miembro en Madrid y al año siguiente en Londres (2005), distintos actos o iniciativas que se fraguaban, recibieron un impulso para su adopción, fortalecimiento y aplicación; por ejemplo, la Orden Europea de Detención y Entrega (Euroorden), Eurojust

³³² CONSEJO EUROPEO (2010), opus cit., p. 28.

(como agencia dedicada a la cooperación judicial internacional, coordinación de las investigaciones y procedimientos), la Red electrónica Judicial Europea, o Europol.»³³³

De forma concisa podemos sostener que la cooperación en Europa se ha llevado a cabo gracias a una serie de instrumentos, jurídicos y no jurídicos, que facilitaron la interrelación tanto entre las instituciones de competencia directa en materia de seguridad (Consejo, Comisión, Parlamento Europeo), como también agencias europeas, órganos preparatorios y grupos de trabajo del Consejo directamente relacionados con estas áreas, quienes, entre otras cosas, “han ido progresivamente perfilando y consolidando el término *radicalización* en el marco de las medidas antiterroristas de la UE.”³³⁴

La institucionalización establecida hasta la fecha se puede simplificar en la siguiente tabla que ilustra, de un modo progresivo, la estrategia de seguridad de la UE en esta materia, y el estrechamiento de los lazos de cooperación entre todos los actores.

La revisión esquematizada permite conocer cómo aquellos instrumentos, normativos y de *Soft Law*, que resultan de especial relevancia en el combate contra el terrorismo, han actuado en el fomento de la cooperación para buscar respuestas multilaterales a las nuevas amenazas, como el actual yihadismo en ciberespacio.

Tabla 3. Evolución de la cooperación en la Estrategia de Seguridad de la UE.

AÑO	INSTRUMENTOS NORMATIVOS Y SOFT LAW	FINALIDAD ESPECÍFICA
2002	Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (DO L 164 de 22.6.2002).	Aproximación a la definición de terrorismo, y base de la política antiterrorista de la UE.
2002	Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.	Coordinación para cooperación judicial en materia penal.
2003	Estrategia Europea de Seguridad (EES, 2003).	Establecimiento de objetivos comunes de seguridad.
2005	Estrategia de la Unión Europea de Lucha contra el Terrorismo (14469/4/05). ▪ Decisión 2005/681/JAI del Consejo, de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI. (<i>Actualmente la Escuela Europea de Policía se denomina Agencia de la Unión Europea para la Formación Policial</i>). ▪ Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que se modifica la Decisión Marco 2002 475/JAI sobre la lucha contra el terrorismo.	Lucha global contra terrorismo mediante 4 pilares: Prevenir (para evitar reclutamiento – La DM 2008/919/JAI se refiere particularmente a los delitos de reclutamiento mediante Internet-), proteger (para evitar atentados), perseguir (más allá de las fronteras de la UE), y responder (coordinar y mejorar las respuestas al fenómeno). La CEPOL es una red que agrupa los centros nacionales de formación de los funcionarios policiales de rango superior con una finalidad de cooperación.
2009	Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008 por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se	Aumentar la eficacia judicial de las autoridades nacionales en la investigación formas graves de delincuencia

³³³ PÉREZ BERNÁRDEZ, Carmela (2012): «La difícil coordinación de la política antiterrorista de la Unión Europea», en: CONDE PÉREZ, Elena (Dir.) /IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, (127-157), p. 131.

³³⁴ RUIZ DÍAZ, Lucas J. (2017): «La prevención de la radicalización en la estrategia contra el terrorismo de la Unión Europea. Entre Soft Law e impulso de medidas de apoyo», *REDI*, vol. 69, 2, p. 259.

	Consejo y se modifica la Decisión 2005/671/JAI del Consejo.	en este ámbito. Sustituye DM 2002/475/JAI como piedra angular de la justicia penal de los países de la UE en la lucha contra el terrorismo, y modifica partes de la DM 2005/671/JAI relativa al intercambio de información y cooperación sobre estos delitos.
2018	Convenio para la Prevención del Terrorismo A. Convenio del Consejo de Europa para la prevención del terrorismo (DOUE L 159/03, 22.6.2018). B. Protocolo adicional al Convenio del Consejo de Europa para la prevención del terrorismo (DOUE de 22 de junio de 2018). C. Decisión (UE) 2018/890 relativa a la celebración, en nombre de la Unión Europea, del Protocolo Adicional al Convenio del Consejo de Europa para la prevención del terrorismo.	Reforzar la lucha contra el terrorismo mediante la cooperación internacional: A) Establece la obligación de conceder asistencia judicial y extraditar entre países y promueve la información espontánea. B) Establece una red de puntos de contacto nacionales activos 24x7 para facilitar el rápido intercambio de información. C) Designa a Europol como contacto para intercambio de información sobre las personas que viajen al extranjero con fines de terrorismo.
2018	Reglamento (UE) 2018/1727 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust), por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo.	Eficacia mediante modificación de la estructura de Eurojust, permitiendo al Colegio de Eurojust concentrarse en mayor medida en aspectos operativos. Considera la creación de la Fiscalía Europea.
2018	Estrategia Contraterrorista del Consejo de Europa (2018-2022).	Establece un mayor proceso de institucionalización antiterrorista en Europa.
2019	EU action to strengthen rules-based multilateralism - Council conclusions (17 June 2019). 10341/19.	Plantea la necesidad actuación de la UE para reforzar el multilateralismo efectivo que promueva los intereses tanto nacionales como colectivos en seguridad y defensa.
2020	Estrategia de la UE para una Unión de la Seguridad (2020-2025)	Refuerza la lucha común contra el terrorismo y la delincuencia organizada. Busca prevenir y detectar las amenazas híbridas y potenciar la resiliencia de las infraestructuras de ciberseguridad. Fomento de la investigación y la innovación en ciberseguridad. Se establecen qué instrumentos y medidas deben desarrollarse en los próximos años para garantizar la seguridad en el entorno físico y digital de Europa.

Fuente: Elaboración propia. 2022.

Existe una línea de actuación cronológica que tiende a evolucionar hacia la especificación en la materia tratada³³⁵ y hacia la cooperación entre los actores de la UE para la seguridad y la defensa.

³³⁵ En la esfera normativa, Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, no proponía definiciones comunes sobre terrorismo, no recogía el concepto de terrorismo de etología religiosa y no consideraba los sistemas informáticos como instrumentos operables por los grupos terroristas para la difusión de propaganda. Por el contrario, la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por

El impulso actual se vertebra en un conjunto de medidas de apoyo que tienden a sostener y fomentar la cooperación en materia judicial y policial. La *Estrategia de la Unión Europea de Lucha contra el Terrorismo* del año 2005 sentó las bases tempranas para el inicio de un trabajo coordinado entre los Estados Miembros, estableciendo su actividad de lucha contra el terrorismo en los cuatro pilares de acción fundamentales denominados *Prevenir, Proteger, Perseguir y Responder*. Las acciones llevadas a cabo por medio de estos pilares se centran en las cuestiones que atañen al terrorismo de etología yihadista que tiene lugar en Internet.

En el pilar de la *prevención*, la UE se emplea actualmente en evitar el reclutamiento y la radicalización por medio de Internet. Para ello, sostiene diversos diálogos, comunicaciones escritas y medidas³³⁶ llevadas a cabo con los EEMM, en donde informa continuamente sobre esta amenaza, y sobre las causas³³⁷ que conducen a la radicalización con el objeto de prevenirlas. La UE contribuye en apoyar a los EEMM en siete ámbitos específicos³³⁸: i) apoyo a la investigación, la constitución de pruebas, el seguimiento y el establecimiento de redes; ii) lucha contra la propaganda terrorista y el discurso del odio en internet; iii) lucha contra la radicalización en los centros penitenciarios; iv) fomento de la educación inclusiva y los valores comunes de la Unión; v) fomento de una sociedad inclusiva, abierta y resiliente y conexión con los jóvenes; vi) lucha contra la radicalización desde la perspectiva de la seguridad; y vii) dimensión internacional. A su vez determina criterios comunes y conceptuales sobre, por ejemplo, lo que entiende la Unión por *radicalización*, y establece soluciones concretas mediante orientaciones prácticas que permitan trabajar de forma coordinada.³³⁹ Por otra parte, el Plan de acción sobre comunicación estratégica³⁴⁰ orienta a los EEMM a trabajar en un contradiscurso elaborado y europeo³⁴¹, tendiente a desarticular y visibilizar la propaganda de terceros.

la que se sustituye la DM 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo, adapta la legislación de la UE en materia penal a las necesidades actuales para luchar contra el terrorismo yihadista. Lo mismo ha sucedido con las iniciativas de *Soft Law*, se ha partido de la Estrategia Europea de Seguridad (EES, 2003), la cual únicamente establecía principios básicos y objetivos comunes de seguridad de la UE, para llegar a comunicaciones específicas en materia de contradiscurso en Internet.

³³⁶ Por ejemplo, el Centro de Excelencia de la Red para la Sensibilización frente a la Radicalización proporciona directrices y manuales para el establecimiento de estructuras multiinstitucionales. Véase: COMUNICACIÓN UE: *Estado de la aplicación de las medidas que figuran en la comunicación de la Comisión sobre apoyo a la prevención de la radicalización que conduce al extremismo violento*, (COM/2016/379 final).

³³⁷ “En el contexto del VII Programa Marco de Investigación y Desarrollo Tecnológico se pusieron en marcha varios proyectos sobre la radicalización. El objetivo de estos proyectos era entender mejor las causas subyacentes a la radicalización y encontrar métodos para evaluar la eficacia de las medidas destinadas a abordarlas. Proyectos de seguridad del VII Programa Marco: www.safire-project.eu; www.impacteurope.eu; www.fp7-prime.eu/project; <http://voxpoleu/>. Proyectos de ciencias sociales y humanidades del VII Programa Marco: «Religious Diversity and Secular Models in Europe - Innovative approaches to Law and Policy» (Diversidad religiosa y modelos seculares en Europa. Enfoques innovadores del Derecho y la Política); «Finding a place for Islam in Europe» (Encontrar un lugar para el islam en Europa); «Combating inequalities through innovative social practices of, and for, young people in cities across Europe» (Combatar las desigualdades mediante prácticas sociales innovadoras de los jóvenes, y para los jóvenes, en ciudades de toda Europa)”. Véase: COMUNICACIÓN UE: *Apoyo a la prevención y radicalización que conduce al extremismo violento* (COM/2016/379 final).

³³⁸ *Ibidem*, p.3.

³³⁹ Miguel Ángel Cano Paños considera que estas soluciones coordinadas tendientes a la prevención deben de tener lugar en un espacio multinivel al enunciar que “[la] prevención de la radicalización no puede constituir únicamente una tarea asignada de forma exclusiva a las fuerzas de seguridad, sino que más bien exige la participación a distintos niveles y con la implicación tanto de profesionales de las ciencias sociales y de la conducta, así como de la sociedad en su conjunto”. Véase: CANO PAÑOS, Miguel Ángel (2018): «La lucha contra la amenaza yihadista más allá del Derecho penal. Análisis de los programas de prevención de la radicalización y des-radicalización a nivel europeo», *Revista de Estudios en Seguridad Internacional (RESI)*, Vol. 4 Núm. 2 (2018), pp. 177-205.

³⁴⁰ Entre otras acciones, el Plan de acción sobre comunicación estratégica (Ares/2015/2608242), solicita a los EEMM que ponga a disposición de sus ciudadanos los dos boletines informativos semanales del Grupo especial sobre comunicación estratégica de la Unión, *The Disinformation Digest* y *The Disinformation Review*, con el fin de sensibilizar a la opinión pública sobre los métodos de propaganda utilizados por terceros.

³⁴¹ EU strategic communications with a view of counteracting propaganda, plantea la necesidad de elaborar un discurso de contraterorismo con una visión comunitaria.

El pilar de la *protección* de la UE se articula por medio de mecanismos de asistencia mutua entre los Estados Miembros y por medio de la asistencia de la UE hacia terceros países a fin de evitar, en este último caso, eventos que repercutan negativamente en el espacio comunitario. Dentro de la Unión existen diversos organismos que trabajan en este pilar, siendo uno de ellos Europol. Europol³⁴², como Agencia de Seguridad de la UE, contribuye a la evaluación de amenazas comunes y define prioridades de actuación operativa en el espacio Schengen. No desarrolla su labor como un cuerpo policial europeo de actuación transnacional, sino que contribuye a la acción de las Autoridades Competentes nacionales, y a la coordinación operativa entre dos o más Estados Miembros, en el caso de los delitos graves transfronterizos como el terrorismo. Luego de siete años de su creación, en el año 2016, se establece un cambio en el marco jurídico de Europol que obliga a los Estados Miembros a cooperar³⁴³ con la Agencia facilitándole toda información que le ayude a cumplir sus objetivos. Debido a ello, Europol ha consolidado un modelo integrado de gestión de datos³⁴⁴ que permite contener toda la información facilitada por los EEMM a fin de procesar la misma mediante verificación cruzada y diversos análisis estratégicos o temáticos. De esta forma se pueden establecer vínculos y conexiones entre varias investigaciones³⁴⁵ y detectar nuevas tendencias y patrones en la delincuencia organizada y el terrorismo. De toda la información registrada y analizada, Europol suministra a los Estados Miembros un Informe anual³⁴⁶ denominado *UE Terrorism Situation & Trend Report* (TE-SAT), en el que figuran cifras de detenciones en la región y nuevas formas delictivas en esta materia.

En un contexto de especificidad mayor, Europol desarrolla el proyecto *Check the Web* (CtW)³⁴⁷ el cual se centra en delitos cometidos a través de Internet³⁴⁸, entre ellos, la distribución de propaganda yihadista, aunque el proyecto no se vincula en exclusiva a esta materia. Para luchar contra el terrorismo Europol establece, en el año 2016, el Centro Europeo Contra el Terrorismo (ECTC), quien dispone de recursos e inteligencia para el Seguimiento de Páginas Web (análisis de material de propaganda en Internet, incluyendo análisis de las amenazas), cuyos datos recabados son incorporados a los Ficheros de Análisis sobre Terrorismo (AWF). Las amenazas detectadas se comparten por medio de la Red de Intercambio de Información (SIENA), que a su vez funciona como una herramienta para permitir la conectividad entre los Estados Miembros y Europol.³⁴⁹

³⁴² Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (EUROPOL)

³⁴³ Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial, art. 7.6.a

³⁴⁴ Exposición de motivos del Consejo: Posición (UE) n.º 8/2016 del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (2016/C 169/02).

³⁴⁵ El modelo integrado de gestión de datos ofrece a su vez mayor certeza jurídica, a fin de no iniciar enjuiciamientos simultáneos y duplicidad de investigaciones en diferentes países de la Unión.

³⁴⁶ En el inciso 3.12 de PANORAMA DE EUROPOL (2012): *Informe general sobre las actividades de Europol*, de 7 de mayo de 2012, (1423-74r2), p. 9, se hace referencia al TE-SAT como el reporte anual en el que se detallan las tendencias del terrorismo en la UE.

³⁴⁷ La función principal de *Check the Web* (Verificar la web) es anticipar y prevenir el abuso terrorista de las herramientas en línea.

³⁴⁸ En el año 2013 comenzó a funcionar dentro de Europol el *European Cybercrime Centre*, EC3. (Centro Europeo de Ciberdelincuencia) que se encarga de coordinar policías nacionales de la UE para combatir los delitos transnacionales cometidos por medio de Internet.

³⁴⁹ Comunicado web del Departamento de Seguridad Nacional de España, Europol pone en marcha el Centro Europeo Contra el Terrorismo (ECTC), en <https://www.dsn.gob.es/en/actualidad/sala-prensa/europol-pone-marcha-centro-europeo-contra-terrorismo-ectc>

En el marco de una cooperación horizontal, se facilita la labor de Agencias y sistemas, como Frontex (Agencia Europea de la Guardia de Fronteras y Costas) o Eurosur (Sistema Europeo de Vigilancia de Fronteras)³⁵⁰ atendiendo a la protección que realizan las mismas sobre las fronteras exteriores de la Unión en relación con los viajes de finalidad terrorista. En este segundo pilar, referente a la protección, cabe destacar el trabajo de CEPOL³⁵¹ como una academia europea de policía para la formación de funcionarios policiales de rango superior de todos los Estados Miembros. Tiende a la unificación de la formación policial potenciando la cooperación en el ámbito de la formación de los servicios responsables del mantenimiento de la ley en la Unión Europea. Para ello busca acrecentar el conocimiento sobre los servicios con los que cuenta la Unión Europea, sobre la terminología técnica en diferentes lenguas, y cuestiones relativas a la ética y los derechos humanos, todo ello enmarcado en un sentimiento de pertenencia comunitario.

El tercer pilar de la UE de lucha contra el terrorismo está centrado en *perseguir*. En el acto de perseguir, incluso más allá de las fronteras de la UE, las formas graves de delincuencia organizada y transfronteriza como lo es el terrorismo, Europol y Eurojust poseen un papel protagónico. La cooperación interinstitucional que tiene lugar entre ambas agencias, y la cooperación que establece a su vez cada agencia con los diferentes Estados Miembros, ha aumentado la eficacia de las acciones policiales y judiciales nacionales para la consecución de fines comunes. Por ejemplo, la orden de detención europea ha resultado ser un instrumento que ha permitido pasar de la cooperación *ad hoc* a la cooperación policial y judicial sistemática, y que ha demostrado ser sumamente eficaz para la persecución e investigación de terroristas más allá de las fronteras nacionales.

Al igual que Europol, Eurojust posee una estrecha relación con autoridades nacionales y organismos de la Unión Europea, tales como la Red Judicial Europea, Frontex, SITCEN³⁵² – por medio de su Unidad Contraterrorista CT-, CEPOL y la Red Europea de Escuelas Judiciales, lo que permite la creación de equipos conjuntos de investigación en el ámbito transfronterizo y un estrechamiento del marco de actuación de las actividades terroristas. Dentro de la Política Criminal de la UE, la investigación conjunta en esta materia tiene por objetivo la eliminación de la actividad terrorista, el impedimento de la planificación terrorista, cortar su financiación, suprimir el acceso a material para la comisión de atentados, y obstaculizar sus redes y actividades en Internet en donde se dediquen a reclutar nuevos terroristas o simpatizantes.³⁵³ Este ámbito delictivo específico dentro del terrorismo, referido a la persecución de la difusión de la propaganda yihadista que incentiva la comisión de atentados, ha implicado el desarrollo de un trabajo progresivo y mancomunado entre los diversos actores europeos.

³⁵⁰ Frontex, Eurosur, el Sistema Electrónico de Autorización de Viaje (ESTA), y el sistema de entrada/salida o Fast Track suponen el establecimiento gradual de un sistema integrado europeo [y de cooperación internacional] de gestión de la frontera exterior de la Unión, en Evolución y desarrollo futuro de la Agencia Frontex y del Sistema Europeo de Vigilancia de Fronteras (Eurosur) (2008/2157(INI)).

³⁵¹ Constituida por Decisión 2005/681/JAI del Consejo, de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI. Desde el 1 de julio de 2016, CEPOL ha pasado a denominarse oficialmente Agencia de la Unión Europea para la Formación Policial (CEPOL), según Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

³⁵² Centro Conjunto de Situación de la Unión Europea.

³⁵³ Estrategia de la Unión Europea de Lucha contra el Terrorismo (14469/4/05).

El cuarto y último pilar se centra en la *respuesta* de la UE a este fenómeno. Para ello se centra específicamente en la coordinación europea a fin de mejorar las respuestas y tratamiento que la Unión otorga al fenómeno terrorista. La interpretación de una respuesta efectiva está estrechamente relacionada con el hecho de aliviar los efectos de las consecuencias de los atentados, de evaluar los hechos sucedidos y de establecer mejores respuestas a futuro para el estrechamiento de la cooperación a los fines de prevención (primer pilar), protección (segundo pilar) y persecución (tercer pilar) del terrorismo yihadista. Este último pilar es fundamental al hecho de que posibilita una autoevaluación de la respuesta de la UE a la amenaza yihadista y la corrección y mejoramiento, siempre en la búsqueda de un mejor resultado, de todas las etapas previas.

La cronología de los diversos instrumentos y estrategias de Unión, así como el desarrollo de los cuatro pilares de lucha contra el terrorismo que se mantienen hasta la fecha, dan cuenta de la búsqueda de un modelo de cooperación entre los diversos actores de la Unión, y también de la necesidad de establecer lazos de cooperación con otros actores del Sistema internacional. Gran parte de la amenaza terrorista contra Europa se origina fuera de la UE, por ello la respuesta debe de tener también una dimensión mundial. La Acción exterior de la UE, principalmente por medio de su unidad EU INTCEN³⁵⁴, proporciona análisis de inteligencia, alerta temprana y conciencia situacional ante las amenazas³⁵⁵ actuales. Esto permite una adecuación de las iniciativas de aplicación interna teniendo en cuenta la dimensión externa, a fin de alimentar los procesos decisorios estratégicos de la UE considerando la importancia del multilateralismo.

MEDIDAS DE VIGILANCIA Y CONTROL DE INTERNET

El uso de las nuevas Tecnologías de la Información y Comunicación (TIC) por parte del yihadismo con fines de reclutamiento, adoctrinamiento y adiestramiento militar es ya un fenómeno ampliamente conocido. La democratización sobre el uso de Internet sentó las bases realistas para el establecimiento de una Sociedad Informacional³⁵⁶ que permita no solo el intercambio de información, sino primordialmente el intercambio y acumulación de ideas que permitan nuevos usos y, entre ellos, usos desvirtuados de su finalidad original.

El uso de la red que realiza el yihadismo para los fines antes descriptos es un segmento ilustrativo de la democratización de Internet dado que en el alcance que supone el uso de las TIC por parte de estos grupos se encuentra una usabilidad no prevista inicialmente que, si bien

³⁵⁴ Centro de Análisis de Inteligencia de la UE (INTCEN) del Servicio Europeo de Acción Exterior (SEAE).

³⁵⁵ Se refiere a las denominadas amenazas híbridas que pueden proceder de grupos terroristas u otros actores. En la COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO (2016): Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea, (JOIN/2016/018 final), se recoge que “*Las campañas de desinformación masiva, que recurren a los medios sociales para controlar el discurso político o para radicalizar, contratar y manipular a individuos que actúan por delegación, pueden constituir vectores de estas amenazas híbridas*”.

³⁵⁶ Se utiliza el término *Sociedad Informacional*, y no *Sociedad de la Información*, debido principalmente al hecho de que este último concepto se centra exclusivamente en un modelo social en el que prima la información. Por el contrario, en la *Sociedad Informacional* de Castells, [...] “*el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la productividad y el poder*.” Véase: CASTELLS, Manuel (2000): *La era de la información: economía, sociedad y cultura. Volumen I: La Sociedad Red*. Madrid: Alianza Editorial, pp. 44-59. Según Castells, lo que caracteriza a la revolución tecnológica actual no es el carácter central del conocimiento y la información, sino la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de la información/comunicación, en un círculo de retroalimentación acumulativo entre la innovación y sus usos. *Ibidem*, p. 46.

no contribuye al incremento tecnológico, si contribuye a una visión innovadora, aunque amenazante del actual uso de la tecnología.³⁵⁷

El uso de Internet con fines yihadistas implica confrontar a la Sociedad informacional con la existencia de grupos terroristas en el ciberespacio³⁵⁸. Sin embargo, existe cierta previsibilidad en este fenómeno, dado que el terrorismo no es un hecho novedoso, sino que ha implicado el desplazamiento de un conflicto previo.³⁵⁹ Como explicábamos anteriormente, en el Capítulo 2, Internet no solo ha permitido la aparición de toda una dimensión de nuevos delitos, sino que ha permitido que los crímenes ya existentes en el mundo real que se encontraban con anterioridad tipificados en legislaciones penales internas, comenzaran a tener también su aparición y desarrollo en el mundo virtual, con su correspondiente reflejo normativo.

Con relación al terrorismo, atendiendo a esta derivación delictiva desde el mundo real hacia el mundo virtual, la Unión Europea se ha empleado a fondo en la tarea de implementar medidas tendientes al control y vigilancia de Internet con el objetivo de prevenir, proteger, perseguir y responder³⁶⁰ el yihadismo en la red.

El Tratado de Lisboa es el instrumento jurídico que, en el marco de la cooperación operativa, ha permitido la creación del Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI). El desarrollo principal de este Comité es la evaluación de amenazas y prioridades nacionales y de la Unión Europea. Entre las diferentes evaluaciones que realiza este Comité junto a otras agencias de la Unión Europea, se estima oportuno el trabajo estratégico para el fomento del desarrollo de nuevas tecnologías desde un enfoque común a fin de acrecentar la eficiencia de la vigilancia en Internet. Dentro de este se busca también incrementar la relación entre el sector público y privado, incentivando los programas de investigación y desarrollo en materia de seguridad cibernética.³⁶¹

Este enfoque estratégico en la Unión Europea respecto a la protección de las actividades terroristas realizadas por medios cibernéticos, y a su vez, el uso de medios informáticos para fortalecer la seguridad en esta materia ha generado una serie de medidas de tipo operativo.³⁶²

³⁵⁷ Nos referimos a los nuevos usos de Internet con una finalidad criminal. En el caso del yihadismo el uso de Internet es especialmente relevante, ya que *“en la mayoría de los casos, Internet es una parte muy importante del proceso de radicalización, ya que intensifica y agiliza dicho proceso. La red global puede proporcionar al usuario la información que está buscando, así como confirmar sus creencias.”* Véase: CANO PAÑOS, Miguel Ángel (2019b): «La violencia terrorista como espectáculo en Internet. Una aproximación criminológica», *Revista Científica General José María Córdova*, 17(28), 2019, p. 692.

³⁵⁸ Orta Martínez se refiere a esto como ciberterrorismo, definiendo este concepto como la convergencia de ciberespacio y terrorismo. Esta conceptualización está limitada a un uso operativo de la red, tales como ataques ilegales y amenazas de ataques contra computadoras, redes y la información almacenada en ellas, cuando son llevados a cabo para intimidar o forzar a un gobierno o a su pueblo en la búsqueda de objetivos políticos y sociales. Véase: ORTA MARTÍNEZ, Raymond (2005), opus cit.

³⁵⁹ Miró Llinares considera que las TIC, en general, e Internet como red global, en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que ha sido denominado ‘El Ciberespacio’, y respecto al cual nos debemos plantear si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o, por el contrario, idéntico a este en sus caracteres esenciales. Véase: MIRÓ LLINARES, Fernando (2011), opus cit., p. 4.

³⁶⁰ Los cuatro pilares de la lucha antiterrorista de la UE descrita en el documento Estrategia de la Unión Europea de Lucha contra el Terrorismo (14469/4/05).

³⁶¹ CONSEJO EUROPEO (2010a), opus cit., p. 28.

³⁶² *“La red global de Internet está siendo actualmente utilizada por el terrorismo islamista como un elemento clave para difundir propaganda, reclutar a potenciales yihadistas, radicalizar, coordinar actividades terroristas y glorificar las atrocidades cometidas por organizaciones como EI [el autodenominado Estado Islámico]. Pero, al mismo tiempo, Internet se ha convertido en la principal fuente de obtención de inteligencia contra el terrorismo. En este sentido, un conjunto creciente de proyectos terroristas ha podido ser desbaratados a través de investigaciones que tuvieron su punto de inicio en el ciberespacio”.* Véase: CANO PAÑOS, Miguel Ángel

Así, por ejemplo, en 11 de enero de 2015, el entonces ministro del Interior de la UE, Bernard Cazeneuve, anunció el inicio de la vigilancia de Internet “en la necesidad de proteger a la población y defender sus derechos”. A tenor de la medida declaró que:

«Internet debe ser un espacio de diversidad, pero respetando la ley, contra todas las manifestaciones de odio y racismo y que intentan seducir mediante la propaganda para crear nuevos terroristas, contra contenidos que hagan apología del terrorismo o llamen a la violencia o al odio.»³⁶³

El marco jurídico del Consejo de Europa³⁶⁴ y de la Unión Europea³⁶⁵ que permite desarrollar esta protección es muy amplio, y se ha ido incrementando conforme los años. De igual forma, el marco jurídico internacional referente a la lucha contra el uso de Internet con fines terroristas comprende una gran variedad de fuentes, entre ellas, las resoluciones de las Naciones Unidas³⁶⁶, los instrumentos jurídicos universales, los acuerdos regionales y las leyes modelo. Todo este constructo político y normativo ha facilitado la implementación de medidas tendientes a la cooperación institucionalizada dentro de la UE para combatir este fenómeno desde dentro mismo de la red.

Luego de los ataques yihadistas en París, en el año 2015, contra el semanario *Charlie Hebdo*, la seguridad en la Unión Europea ha cobrado mayor importancia y la cooperación se ha intensificado. Desde entonces Internet está siendo profundamente monitoreado y las compañías de servicios tecnológicos están sujetas a una serie de regulaciones y compromisos de seguridad. ENISA³⁶⁷ desempeña un papel determinante en este ámbito, atendiendo a las vulnerabilidades de las redes europeas, no solo en cuanto a su infraestructura, sino también a contenidos en Internet que vulneren principios democráticos. ENISA también desempeña un papel fundamental en las actuaciones de Eurojust, en lo referente a la determinación de la jurisdicción y territorialidad³⁶⁸ de los proveedores de servicios digitales europeos al establecer pautas relativas al establecimiento de la empresa.

En un afán persecutorio, más allá de sus fronteras exteriores, la Unión Europea extiende su marco regulatorio a los proveedores de terceros países.³⁶⁹ Eso significa que dentro y fuera de la

(2019c): «La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico», *Revista Científica General José María Córdova*, 17(26), 2019, p. 278.

³⁶³ «La Unión Europea reforzará el control de fronteras e Internet», *Diario de Navarra*, edición online de 11 de enero de 2015. Disponible en: <https://www.noticiasdenavarra.com/mundo/2015/01/11/ue-reforzara-control-fronteras-exteriores-2930972.html> [Fecha de consulta: 03 de noviembre 2023].

³⁶⁴ CONSEJO DE EUROPA (2003), opus cit.

³⁶⁵ Entre toda la normativa y la estrategia político-institucional enunciada relativa a la lucha contra el terrorismo elaborada por la Unión Europea, merecen especial atención la Decisión Marco 2002/475/JAI y la Decisión Marco 2008/919/JAI por el aporte legislativo y la búsqueda de armonización.

³⁶⁶ Las resoluciones de las Naciones Unidas resultan sumamente relevantes. Por ejemplo, “*Las resoluciones del Consejo de Seguridad pueden imponer obligaciones jurídicamente vinculantes para los Estados Miembros o proporcionar fuentes de compromisos políticos de derecho incipiente.*” Véase: UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012), opus cit., p. 17.

³⁶⁷ Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad). ENISA colabora no solo con todos los actores de la UE, sino también con organismos internacionales, como la OCDE, OSCE y OTAN a fin de detectar ciberamenazas, (art. 42).

³⁶⁸ Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, (art. 18).

³⁶⁹ Esto es especialmente relevante debido al hecho de que gran parte de la actividad propagandística por parte del yihadismo que tiene por objetivo Europa, se encuentra alojada en prestadores de servicios digitales con establecimiento fuera de la Unión. En el caso de Estados Unidos, la protección a la libertad de expresión amparada en la Primera Enmienda dificulta las actuaciones de la UE.

Unión, actualmente los usuarios, los proveedores de Internet y las empresas privadas de servicios de comunicación, están siendo monitoreados en virtud del uso terrorista que algunos usuarios realizan de Internet.

El progresivo uso terrorista de las redes sociales y otras plataformas de comunicación con el fin de promover la propaganda del yihadismo, la captación de nuevos miembros, y la radicalización, así también para la implementación de otro tipo de acciones en la red tendientes a acrecentar la ideología terrorista del yihadismo global y el número de atentados cometidos, ha supuesto un monitoreo de Internet sin precedentes. La vigilancia y el control de Internet orientado a prevenir delitos de naturaleza terrorista está siendo, en la última década, más activa que nunca. Sin embargo, toda esta ingente labor no está exenta de dificultades técnicas. Según Eurojust “el uso de Internet para propósitos terroristas crea una carga adicional [de trabajo] para la investigación y el procesamiento de combatientes extranjeros”³⁷⁰, ello en virtud de que, conforme a esta agencia, “la interceptación de comunicaciones por voz sobre protocolo de Internet (como por ejemplo Skype, Viber, etc.) es problemática y dificulta seriamente las investigaciones”³⁷¹

A fin de dotar esta labor con organismos eficaces, y atendiendo a una Política Criminal Europea coordinada y preventiva, tiene lugar en este contexto la creación de la Unidad de Referencia de Internet de la UE (EU IRU)³⁷². La EU IRU se crea a petición del Consejo de Justicia y Asuntos de Interior, quien solicitó, en el año 2015, a Europol una respuesta operativa para poner freno al creciente e incontenible número de sitios web en Internet con contenido yihadista.³⁷³

La función de la Unidad de Referencia de Internet (EU IRU) es detectar, alertar de forma temprana e investigar las acciones delictivas en portales de Internet y en redes sociales. Para ello monitorea la red 24x7 a fin de detectar amenazas terroristas. En su monitoreo realiza búsquedas dirigidas en Internet con palabras claves y metadatos. “Estas búsquedas también se realizan en la *Dark Web*, redes a la que se sólo se puede acceder con programas específicos donde proliferan actividades delictivas de todo tipo.”³⁷⁴ No solo previene crímenes de índole terrorista, sino que también proporciona medios de prueba para formalizar ulteriores investigaciones judiciales. Existen cuatro vectores principales sobre los que trabaja la EU IRU. Estos vectores son: 1) Soporte a investigaciones: suministra información y brinda asistencia a instituciones y agencias de la UE y a EEMM, a fin de ayudar en el cumplimiento de los objetivos estratégicos propuestos en la lucha contra el terrorismo yihadista; 2) Análisis y referencias: identifica publicaciones terroristas pertenecientes al yihadismo y a otras formas de extremismo

³⁷⁰ Se refiere a posibles terroristas con pasaporte europeo, que habiendo sido entrenados y radicalizados fuera del espacio Schengen, retornan a la Unión Europea con la finalidad de cometer actos terroristas o criminales dentro del territorio de la Unión.

³⁷¹ «UE debe aceptar intervenir Skype para evitar vuelta de insurgentes», *Noticia de Reuters*, edición online de 06 de febrero de 2015. Disponible en: <https://www.reuters.com/article/oesen-ue-skype-seguridad-idESKBN0LA1QM20150206/> [Fecha de consulta: 29 de noviembre de 2023].

³⁷² EU IRU por sus siglas en inglés (*EU Internet Referral Unit*, -Unidad de Referencia de Internet de la Unión Europea-). Véase: Unidad de Referencia de Internet de la Unión Europea, *Europol*. Disponible en: <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referral-unit-eu-iru> [Fecha de consulta: 29 de noviembre de 2023].

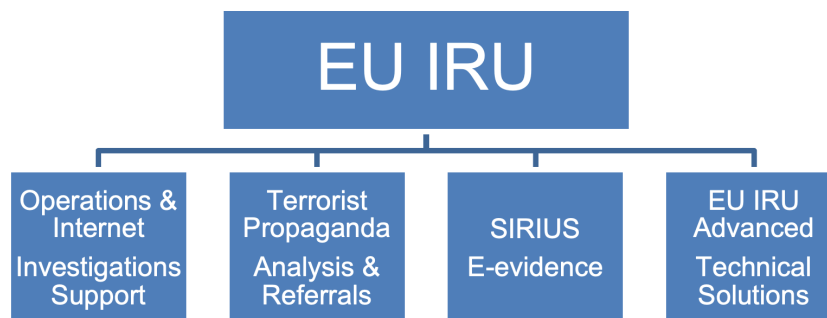
³⁷³ La Unidad de Referencia de Internet (EU IRU) no solo posee la función de detectar y eliminar las publicaciones yihadistas online. También se centra en eliminar el contenido violento de la extrema derecha. Debido a los atentados de Christchurch (Nueva Zelanda) en el año 2019, ha habido un incremento de las publicaciones de la extrema derecha en Internet. La EU IRU también da su asistencia al Centro Europeo de Contrabando de Migrantes de Europol identificando contenido propio de los servicios ilegales de contrabando a migrantes y refugiados.

³⁷⁴ UNIDAD DE REFERENCIA DE INTERNET (2019): Informe de actividad 2019 de la Unidad de Referencia de Internet de la Unión Europea, Europol, 25 de octubre 2020. Disponible en: <https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-actividad-2019-unidad-referencia-internet-iru-union-europea> [Fecha de consulta: 29 de noviembre de 2023].

político³⁷⁵ en línea; 3) SIRIUS³⁷⁶: colabora con autoridades judiciales y policiales de EEMM y con socios de la UE compartiendo información relevante respecto a material delictivo en la red,³⁷⁷; y, 4) Soluciones técnicas: solicita a proveedores de servicios de Internet la eliminación de contenidos terroristas o extremistas, y ofrece colaboración a dichas empresas proveedoras de servicios de Internet.

De acuerdo con el Departamento de Seguridad Nacional de España, la composición de EU IRU es la siguiente:

Gráfico 6: Estructura de EU IRU



Fuente: DSN España

El trabajo de EU IRU se desarrolla de forma permanente en estos cuatro campos de acción a fin de fomentar la cooperación en el control y vigilancia de Internet.

De acuerdo con un especialista de la Unidad, la vigilancia de Internet es:

«[...] una operación de 24 horas [...] una vez que identificamos el contenido terrorista en sí, tratamos de mapear su rastro en Internet. Recopilamos toda la información disponible públicamente sobre este contenido y creamos un ‘paquete de referencia’ para ser explotado con diferentes propósitos: evaluar la amenaza, respaldar las investigaciones y sugerir una posible remisión a proveedores de servicios en línea. La remisión es la transmisión de una notificación de contenido de Internet por parte de Europol o los Estados Miembros a los proveedores de servicios en línea.»³⁷⁸

Dentro de su estructura, la EU IRU posee especialistas con una gran variedad de habilidades que le permiten desarrollar sus actividades, incluso de forma coordinada. Dichos especialistas están organizados en cuatro equipos separados con experiencia operativa, lingüística, técnica y de investigación. Por ejemplo, los especialistas en el idioma árabe son contratados no sólo por sus capacidades idiomáticas, sino también por su entendimiento del islam y de la fundamentalización religiosa para la captación y la radicalización del yihadismo. Conforme a un especialista de EU IRU “el idioma es muy importante en el fenómeno del yihadismo, [...]”

³⁷⁵ Nos referimos aquí a las publicaciones online de la extrema derecha y de la extrema izquierda.

³⁷⁶ Acceso Transfronterizo a la Prueba Electrónica (Cross Border Access to Electronic Evidence)

³⁷⁷ “SIRIUS es un proyecto financiado por la UE que ayuda a las autoridades judiciales y policiales a acceder a pruebas electrónicas transfronterizas en el contexto de investigaciones y procedimientos penales.” Disponible en: <https://www.europol.europa.eu/operations-services-innovation/sirius-project#:~:text=SIRIUS%20is%20an%20EU%2Dfunded,of%20criminal%20investigations%20and%20proceedings>. [Fecha de consulta: 03 de noviembre de 2023].

³⁷⁸ «Europol explica cómo combate la difusión de contenidos terroristas en internet», *Escudo Digital*, edición online de 4 de febrero de 2022. Disponible en: https://www.escudodigital.com/ciberseguridad/europol-bases-combatir-contenidos-terroristas-internet_50273_102.html [Fecha de consulta: 29 de noviembre de 2023].

pero también hay que tener un conocimiento profundo de cómo las redes yihadistas abusan del entorno online para reclutar y radicalizar a las personas”.³⁷⁹

Otro miembro de EU IRU expresa al respecto:

«Somos un equipo con personas de diferentes orígenes. Tenemos a los investigadores antiterroristas; Contamos con expertos en TI, expertos en comunicación, investigadores con experiencia en jurisprudencia islámica y también en estudios de área. También tenemos lingüistas; cubrimos la mayoría de los idiomas europeos además de árabe, ruso y turco. Así, intentamos combinar este conjunto de habilidades para comprender tanto el contenido del mensaje como la difusión de la propaganda.»³⁸⁰

La EU IRU desarrolla lo que se conoce como *Referral Action Days* (RADs)³⁸¹. Los *Referral Action Days* son jornadas que se realizan de forma periódica y que se llevan a cabo en las instalaciones de Europol y también a distancia. Estos RADs facilitan la cooperación directa con los representantes de los Cuerpos y Fuerzas de Seguridad de los EEMM, y por ello resultan imprescindibles en la lucha que realiza Europol contra el terrorismo yihadista. Desde el año 2015 hasta noviembre de 2021 la EU IRU ha organizado un total de 23 RADs.³⁸²

En relación con el trabajo realizado en el marco de los RADs, en noviembre de 2021, un especialista de EU IRU, expresaba:

«[...] este es un momento histórico porque toca los aspectos fundamentales de los derechos humanos y las libertades. Por un lado, debemos estar seguros, como europeos, de que no impactamos estos derechos y securitizar el área; pero al mismo tiempo tenemos que tomar medidas reales para controlar el abuso de Internet por parte de actores malintencionados. Es un equilibrio difícil de alcanzar, pero hay que hacerlo.»³⁸³

El monitoreo del contenido terrorista en línea ha llevado no solo a la creación de la Unidad de Referencia de Internet de la UE (EU IRU), sino también a la adopción de nuevas medidas de tipo normativo. El Reglamento UE (2021) /784³⁸⁴ aborda la difusión de contenido terrorista en línea. Para ello, busca luchar “contra el uso indebido de los servicios de alojamiento de datos con fines terroristas y contribuyendo a la seguridad pública en toda la Unión”³⁸⁵

En las consideraciones previas del Reglamento se reconoce que las acciones terroristas del yihadismo en la red poseen un impacto negativo en la sociedad, y se destaca la importancia de las empresas privadas proveedoras de Internet en la promoción del terrorismo en Internet.

³⁷⁹ «Operación de Europol dirigida al contenido terrorista en línea», *OIPOL*. Disponible en: <https://oipol.org/2022/02/03/operacion-de-europol-dirigida-al-contenido-terrorista-en-linea/> [Fecha de consulta: 29 de noviembre de 2023].

³⁸⁰ EUROPOL EU IRU OFFICIAL (2020): «A View from the CT Foxhole: An Interview with an Official at Europol’s EU Internet Referral Unit/Entrevistado por A. Amarasingam», *CTC Sentinel, Combating Terrorism Center at West Point*, edición online de febrero 2020. Disponible en: <https://ctc.westpoint.edu/view-ct-foxhole-interview-official-europol-eu-internet-referral-unit/> [Fecha de consulta: 01 de noviembre de 2023]. Nota: Entrevista [en inglés] realizada el 11 de diciembre de 2019 a un especialista de EU IRU acerca de la relación actual de Europol con las empresas de redes sociales y el desafío continuo de la UE para combatir el contenido terrorista en línea. El funcionario solicitó el anonimato. Europol ha revisado la entrevista y ha aprobado su publicación.

³⁸¹ RADs por sus siglas en inglés (*Referral Action Days*, -Días de Acción de Referencia-).

³⁸² El periodo de tiempo que contabiliza los 23 RADs a los que se hacen referencia es el que va desde el nacimiento de la Unidad de Referencia de Internet (EU IRU) hasta la fecha de publicación del artículo citado. Véase: «How is Europol keeping online spaces safe?», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/how-europol-keeping-online-spaces-safe> [Fecha de consulta: 29 de noviembre de 2023].

³⁸³ «Operación de Europol dirigida al contenido terrorista en línea», *Ibidem*.

³⁸⁴ REGLAMENTO (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea.

³⁸⁵ *Ibidem*, art. 1.

Debido a ello se insta a que las empresas asuman la responsabilidad del importante papel que les toma cumplir en este escenario criminal y se recoge que:

«[...] la presencia de contenidos terroristas en línea ha demostrado ser un catalizador para la radicalización de individuos que puede conducir a la comisión de actos terroristas y, por tanto, tiene graves consecuencias negativas para los usuarios, los ciudadanos y la sociedad en general, así como para los prestadores de servicios en línea que alojan esos contenidos, dado que menoscaba la confianza de sus usuarios y daña sus modelos de negocio. En vista de su papel esencial y de los medios y capacidades tecnológicas asociados a los servicios que prestan, los prestadores de servicios de alojamiento de datos tienen la responsabilidad social particular de proteger sus servicios del uso indebido por parte de los terroristas y a ayudar a luchar contra la difusión de contenidos terroristas a través de sus servicios en línea, teniendo en cuenta la importancia fundamental de la libertad de expresión, incluida la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática.»³⁸⁶

Por medio del Reglamento UE (2021) /784 se faculta a la UE y a los EEMM para instar a las empresas privadas a que retiren de Internet el contenido identificado como yihadista, luego de que la Unidad de Referencia de Internet haya alertado de su existencia tras los periódicos monitoreos de la red.

Con el objeto de establecer definiciones en el área y de facilitar la colaboración de las empresas ante el temor por parte de estas de incurrir en actos de censura, este Reglamento a todo efecto adopta la definición de “contenidos terroristas”³⁸⁷ que se haya recogida con anterioridad en la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo.³⁸⁸ Este cambio legislativo que introduce el Reglamento UE (2021) /784 así también como la colaboración gestada entre la UE y las empresas proveedoras de servicios de Internet ha generado un salto evolutivo en cuanto a la vigilancia y monitoreo de la red, porque permite que tanto la Unión Europea, así también como los Estados Miembros a título particular, puedan comenzar a exigir a, partir del año 2022, a las empresas de tecnología la eliminación de contenido online de sus propios servidores sin por ello debilitar los derechos y libertades fundamentales. Un especialista de Europol resumía este equilibrio entre seguridad y derechos fundamentales en la siguiente declaración:

«En la IRU de la UE, el Centro Europeo contra el Terrorismo y, en términos más generales Europol, respetamos los derechos y libertades fundamentales dentro de un marco legal sólido, [...] y es por ello que la comunidad internacional, las empresas con las que colaboramos, y los Estados Miembros confían en nosotros. Estamos muy comprometidos en generar esta confianza, y la confianza es nuestro mayor logro en Europol.»³⁸⁹

La adopción del Reglamento UE (2021) /784 cambia por completo la relación de trabajo del Centro Europeo contra el Terrorismo con los Estados Miembros y las empresas tecnológicas porque se pasa de una acción voluntaria entre las partes a una acción obligatoria, operativa y coordinada por Europol. Esta coordinación se lleva a cabo por medio de la plataforma PERCI.³⁹⁰ Según un artículo de la oficina de prensa de la Agencia:

³⁸⁶ *Ibidem*, Consideración previa N.º 5.

³⁸⁷ *Ibidem*, Consideración previa N.º 11.

³⁸⁸ Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión Marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

³⁸⁹ «How is Europol keeping online spaces safe?», *Ibidem*.

³⁹⁰ Plataforma Europea para Eliminar Contenidos Ilegales en Internet (*Plateforme Européenne de Retraits de Contenus illégaux sur Internet*).

«Esta plataforma es una solución técnica construida por Europol y gestionada por IRU de la UE para facilitar la implementación del nuevo reglamento. Antes de esto, el proceso para eliminar contenido terrorista en línea era totalmente voluntario por parte de las empresas de tecnología.»³⁹¹

A partir de esta adopción normativa, la IRU de la UE se encuentra en una posición única que le permite mapear redes terroristas a través de las fronteras y ver cómo están vinculadas con casos en una variedad de Estados Miembros. Es esta visión global la que resulta fundamental para dismantelar las redes criminales y proporcionar información para las investigaciones.

El nuevo escenario legal y la interacción operativa institucionalizada entre gobierno, empresas de tecnología y sociedad civil para contrarrestar el terrorismo en línea y el extremismo violento representa un gran logro dentro de la Política Criminal de la UE en relación con el terrorismo yihadista en Internet porque da inicio a la asociación público-privada en esta materia.

La asociación público-privada propiciada a iniciativa de Europol, ha permitido que comenzaran a llevarse a cabo diversos *Referral Action Days* (RADs), no solo con integrantes de instituciones de la UE y representantes de EEMM, sino también, y ello ha significado un cambio determinante en los RADs, con empresas de tecnología y servicios de Internet.

El 21 y 22 de noviembre de 2019, la EU IRU organizó en su sede de La Haya las 16.^a Jornadas de Acción de Referencia conjuntas.³⁹² A esta acción se sumaron un total de nueve proveedores de servicios online, entre ellos *Telegram*³⁹³, *Google*³⁹⁴, *Files.fm*³⁹⁵, *X*³⁹⁶, e *Instagram*³⁹⁷. El trabajo de EU IRU se basó en identificar contenido yihadista en la red y referenciarlo a los responsables de las empresas para su evaluación interna a fin de establecer cualquier posible incumplimiento de los términos de servicio de la compañía. Entre las publicaciones referenciadas se encontraban vídeos de propaganda yihadista, publicaciones de organizaciones terroristas, y cuentas de redes sociales que promovían el terrorismo y el extremismo violento. A su vez, en el marco de este RAD, de modo particular EU IRU y *Telegram* participaron conjuntamente en el desarrollo de una campaña de interrupción de los canales y grupos del

³⁹¹ Véase Índice: ANEXOS. Anexo N.º 02: Documento público funcionamiento interno de PERCI.

³⁹² «Referral Action Day against Islamic State online terrorist propaganda», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda> [Fecha de consulta: 01 de diciembre de 2023].

³⁹³ Plataforma online, de origen ruso, de servicios de mensajería instantánea y VoIP (*Voice over IP*, - voz sobre IP-, que significa servicios transmisión digital de audio y video). Permite el alojamiento de archivos. Se encuentra disponible desde agosto de 2013 y opera en más de 14 idiomas.

³⁹⁴ *Google* LLC (1998, origen California, EE.UU.) es una empresa de tecnología. Desarrolla su trabajo centrado en la inteligencia artificial, publicidad en línea, motores de búsqueda, computación en la nube, software, informática cuántica, comercio electrónico y datos de consumo.

³⁹⁵ Empresa de TI, fundada en 2008, desarrolladora de software y soluciones de almacenamiento de datos en la nube para empresas y usuarios privados desde 2007. Permite almacenar, compartir o enviar datos de forma segura. Permite la transmisión de grandes volúmenes de contenido sin pérdida de calidad.

³⁹⁶ Anteriormente *Twitter*. Denominado en el circuito de tecnología como el ‘SMS de Internet’, se ha fundado en el año 2006 en San Francisco, CA, EE.UU. Es una empresa de comunicaciones en la industria de Internet cuya red social gratuita de microblogging sirve para enviar mensajes cortos, de hasta 280 caracteres.

³⁹⁷ *Instagram* es una aplicación y red social de origen estadounidense. Su desarrollador, la compañía de tecnología y redes sociales Meta (conocida anteriormente como *Facebook*, Inc., con sede en Cambridge, Massachusetts, EE.UU.), estableció su lanzamiento al mercado en octubre de 2010.

Estado Islámico en la plataforma de esta empresa.³⁹⁸ Esta acción coordinada se centró en promover la restricción de la difusión de contenidos terroristas online.

Aún cuando se han desarrollado RADs con intervención privada de forma previa, y EU IRU se encontraba trabajando en colaboración con *Telegram* desde hacía ya más de un año (existe un RAD con la compañía en octubre de 2018³⁹⁹), el RAD de noviembre de 2019 fue el primero que ha tenido mayor alcance e impacto⁴⁰⁰ en la relación con esta empresa, debido al hecho de que mediante las acciones llevadas a cabo durante esos días cientos de canales de los principales medios de propaganda de los yihadistas, como *Quraysh Media*, *Kilafah News*, *Nashir* o la Agencia de noticias *Amaq*, (perteneciente al Estado Islámico) fueron expulsados para siempre de la plataforma de *Telegram*.⁴⁰¹

Sí bien con *Google* e *Instagram* durante este RAD se trabajó también en la identificación y eliminación de contenido de Internet de publicaciones terroristas, fue con la empresa *Telegram* con la que, en esta jornada, el trabajo ha dado sus mayores resultados, debido principalmente a que *Telegram* fue la última empresa de tecnología en incorporarse a esta modalidad de colaboración con Europol, por lo tanto gran parte del contenido yihadista que ya había sido eliminado de las plataformas de las otras empresas, aún se encontraba disponible en esta compañía.⁴⁰² En dicho RAD, se revisó no solo la propaganda yihadista sino también aquella que era considerada propia del extremismo ideológico más violento existente en Internet, y que forma parte de *Terrorgram*.⁴⁰³ Tomando en consideración la magnitud del material analizado en este RAD, la labor conjunta entre *Telegram* y Europol, ha sido todo un éxito.

³⁹⁸ «Europol and Telegram take on terrorist propaganda online», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online> [Fecha de consulta: 01 de diciembre de 2023].

³⁹⁹ En este RAD celebrado el 3 de octubre de 2018, y que contó con la presencia de algunos EEMM (Bélgica, Francia, Alemania, Italia, Países Bajos y Reino Unido*), *Telegram*, asistió a solo una parte del evento, para permitirle a EU IRU revisar conjuntamente el contenido detectado y difundido en línea por grupos terroristas. Esta acción coordinada contra la propaganda terrorista en línea se centró en la producción en línea de material terrorista por parte de Estado Islámico y medios de comunicación afiliados a Al Qaeda. Entre los elementos remitidos se encontraban archivos (PDF, videos y audios) con material terrorista y canales públicos de Telegram que alojan este material. Cabe recordar, que aún luego de la revisión conjunta, la eliminación final del material referido en los servidores es una acción voluntaria por parte de cada empresa en cuestión y se ajusta a los propios términos y condiciones de la misma. *Nota: A fecha del citado RAD, Reino Unido era Estado Miembro de la Unión Europea, dado que no había tenido lugar aún el *Brexit*. No obstante, en los futuros RADs debe observarse que Reino Unido ya no pertenece a la UE, aunque ello no impide que mantenga su colaboración con Europol y en los *Referral Action Days*.

⁴⁰⁰ «Se trata de la operación más completa y amplia contra la 'yihad online' del Estado Islámico desde que los yihadistas encontraron su refugio ideal en Telegram a partir de 2015. Las cifras son apabullantes: en un solo día a finales de noviembre (el 27), se suspendieron de golpe 10.345 cuentas, canales o contenido terrorista, en un mes en el que no se pasaba de una media de menos de 100 suspensiones diarias. El día 21, la tendencia comenzó a cambiar: en tres días, se eliminaron 2.096, 2.959 y 3.516 cuentas, canales y contenidos terroristas, según cifras de ISIS Watch.» Véase: «El ISIS busca nueva plataforma: la Europol asedia su propaganda en Telegram», *El Confidencial*, edición online de 3 de diciembre de 2019. Disponible en: https://www.elconfidencial.com/mundo/2019-12-03/ahogado-por-telegram-el-isis-busca-otras-aplicaciones-para-seguir-con-su-propaganda_2362587/ [Fecha de consulta: 02 de diciembre de 2023].

⁴⁰¹ «Los canales, conocidos colectivamente como Agencia de Noticias Nashir, promocionaron [en Telegram] enlaces de al menos ocho canales duplicados en TamTam. [...] «Los canales TamTam actúan como espejo de los canales de la Agencia de Noticias Nashir en Telegram, que difunden propaganda oficial del EI.» Véase: «Messaging app TamTam used for IS propaganda dissemination», *BBC Monitoring*, edición online de 07 de Abril de 2018. Disponible en: <https://monitoring.bbc.co.uk/product/c1dp1q1i> [Fecha de consulta: 02 de diciembre de 2023].

⁴⁰² Sí bien el grueso del trabajo se centró en la colaboración Europol-Telegram para identificación y erradicación de contenido yihadista, Google y YouTube, dos empresas que fueron de las primeras en colaborar voluntariamente con EU IRU, acudieron a la sede de Europol para un intercambio de expertos, continuando la cooperación continua de las empresas en la lucha contra el terrorismo en línea. Véase: «Referral Action Day against Islamic State online terrorist propaganda», *Ibidem*.

⁴⁰³ *Terrorgram* es un neologismo acrónimo que remite a un conjunto de canales y cuentas de *Telegram* que promueven el extremismo político neo-Nazi (la cultura de *Siege*). Sus miembros poseían en *Telegram* guías sobre cómo fabricar explosivos, manifiestos de supremacistas blancos, videos de grupos neonazis, incluida la División Atomwaffen, la Orden Nacionalsocialista, La Base y la División Feuerkrieg. Al menos siete canales publicaron un libro neonazi que incita a la violencia del actor solitario, la violencia

Al respecto de estos dos días de trabajo conjunto, el representante de *Telegram* enunció:

«Los Días de Acción de Referencia nos parecieron productivos y útiles. Apoyamos la libertad de expresión y las protestas pacíficas, pero el terrorismo y la propaganda de violencia no tienen cabida en *Telegram*. Estamos mejorando constantemente nuestros procedimientos internos y herramientas de moderación para garantizar que nuestra plataforma se mantenga libre de abusos. [...] *Telegram* no es un lugar para la violencia o la actividad criminal.»⁴⁰⁴

Bajo esta premisa la empresa ha comenzado a esforzarse en reforzar su capacidad técnica⁴⁰⁵ para contrarrestar el contenido yihadista, a la vez que estrecha su asociación con la UE y su agencia Europol.

El 1 de febrero de 2022, tuvo lugar otro RAD cuyo punto focal de análisis conjunto ha sido nuevamente el contenido yihadista online. La coordinación de esta actividad estuvo a cargo también de la Unidad de Referencia de Internet de la UE (EU IRU), y contó con la participación de delegaciones nacionales especializadas en la lucha contra el terrorismo de Francia, Alemania, Hungría, Italia, los Países Bajos, Portugal, España, Suiza y Reino Unido. En esta operación de monitoreo se evaluaron 106 páginas webs en las cuales se promovía la ideología del terrorismo yihadista, así como discursos extremistas de violencia política. De estas páginas webs se extrajeron 563 publicaciones⁴⁰⁶, para posteriormente poner dicha información en conocimiento de las empresas proveedoras de servicios a fin de solicitar el retiro voluntario de dicho contenido conforme a los términos y condiciones de uso de la propia empresa.⁴⁰⁷

Al igual de lo que sucede con las empresas privadas, la participación de los Estados Miembros en los RADs es crucial. En el caso de los EEMM, ya no solo por su condición de miembro de la UE, sino también porque los EEMM pueden establecer mecanismos judiciales internos hacia las empresas que sean reticentes a colaborar y que resulten dentro del ámbito de su competencia. Recordemos que la EU IRU no está facultada para obligar a las compañías a suspender o eliminar definitivamente el contenido yihadista (de acceso público o privado) de sus servidores, debido a que su función principal respecto al contenido yihadista en Internet se centra en identificar y referenciar dicho material terrorista hacia las empresas, a fin de que estas obren de forma voluntaria y colaborativa. El procedimiento sería el siguiente:

en el lugar de trabajo, ataques a infraestructuras, a Fuerzas del orden, políticos, gente de color, judíos, musulmanes, Sikhs, latinos y personas LGBTI. El libro también incluye información sobre cómo fabricar bombas caseras, realizar vigilancia, e información útil para cometer ataques. Véase: «Extremist Content Online: TamTam Edition. Messenger Platform Is Home To Content Promoting Neo-Nazi Accelerationism And Acts Of Terrorism», *Counter Extremism Project (CEP)*. Disponible en: <https://www.counterextremism.com/press/extremist-content-online-tamtam-edition> [Fecha de consulta: 01 de diciembre de 2023].

⁴⁰⁴ «Extremist Content Online: TamTam Edition. Messenger Platform Is Home To Content Promoting Neo-Nazi Accelerationism And Acts Of Terrorism», *Ibidem*.

⁴⁰⁵ Telegram ha ampliado las herramientas a disposición de los usuarios de control de contenido. «*Ahora, cualquier usuario puede referir y clasificar el contenido que considere inapropiado y violento a través de la función de referencia en grupos y canales públicos. Además, los nuevos desarrollos técnicos, como el avanzado sistema automatizado de detección de contenido, continúan fortaleciendo aún más el esfuerzo de Telegram por erradicar aún más el extremismo en la plataforma*». Véase: «Europol and Telegram take on terrorist propaganda online», *Ibidem*.

⁴⁰⁶ Principalmente manuales y/o tutoriales que aconsejaban sobre la utilización de precursores de explosivos para la fabricación de bombas a fin de que sean utilizadas en atentados terroristas.

⁴⁰⁷ Cabe señalar que no existe acuerdo de colaboración con todas las empresas y/o plataformas de redes sociales, quedando por tanto a discreción de la propia empresa el retiro de la información identificada por EU IRU. No obstante, la gran mayoría de las empresas de tecnología han tomado medidas, en sus términos y condiciones de uso, orientadas a protegerse de publicaciones de índole terrorista.

«Una vez localizado este tipo de mensaje, la IRU remite esta información a los distintos proveedores de servicios de internet, principalmente a través del Foro de Internet de la UE (EUIF) y del Foro mundial de Internet sobre la lucha contra el terrorismo (GIFCT), para que procedan a su eliminación.»⁴⁰⁸

No obstante, un EEMM motivado en algún fundamento de urgencia por inminente riesgo dentro de su territorio, o por extrema relevancia, puede activar los mecanismos legales que le permite su legislación nacional a fin de incrementar su seguridad y con ello también la del resto del espacio Schengen.

Es por todo ello por lo que resulta de máxima relevancia la participación de los EEMM en los RADs. Al respecto, del trabajo recíproco entre las partes en este ámbito un especialista de EU IRU menciona:

«[...] Cuando se trata de investigaciones, apoyamos a los Estados Miembros con información disponible públicamente. No tenemos acceso a información cerrada. Los Estados Miembros deben utilizar sus instrumentos legales para solicitar acceso a este tipo de información a las empresas de redes sociales. Básicamente, si hay una investigación abierta por parte de los Estados Miembros y obtienen acceso a este tipo de contenido, pueden acudir a nosotros para realizar un análisis más detallado. Pero no tenemos la base legal para solicitar a las empresas de redes sociales que nos revelen datos que no estén disponibles públicamente.»⁴⁰⁹

Además de brindar información para las diligencias judiciales internas, la EU IRU produce conocimientos estratégicos sobre el terrorismo yihadista y brinda apoyo a las autoridades policiales de los Estados Miembros de la UE para sus investigaciones criminales en línea.

La evolución a lo largo de los años del trabajo dentro de la EU IRU puede comprenderse a partir de la lectura del siguiente extracto de la entrevista de *Combating Terrorism Center at West Point* (CTC)⁴¹⁰ realizada en diciembre de 2019. En ella, a un especialista anónimo de EU IRU declara que:

«[La razón para crear EU IRU] fue tener una mejor comprensión del panorama de amenazas, especialmente cuando se trata de la amenaza que representan estas organizaciones designadas como terroristas para Europa [...] luego se hizo cada vez más evidente que necesitábamos desarrollar esta capacidad y también tener un mandato para apoyar a los Estados Miembros con investigaciones en línea en el contexto de la lucha contra el terrorismo, [además] desde el primer día, comenzamos a colaborar con proveedores de servicios en línea para señalarles contenido terrorista y encontrar soluciones sobre cómo interrumpir la difusión de contenido. [Al comienzo,] recuerdo que la mayor parte de la propaganda estaba en las principales redes sociales como *Twitter* o *Facebook*. Priorizamos este tipo de plataformas para trabajar juntas y su respuesta fue muy positiva. Basamos esto en un enfoque voluntario. Básicamente, comenzamos nuestras operaciones para monitorear contenido terrorista, es decir, contenido de marca, producido y difundido por organizaciones terroristas designadas, y al rastrear este contenido a través de Internet, estábamos en condiciones de señalarlo también en línea. Entonces, comenzamos a señalar este tipo de contenido a las empresas de redes sociales y entablamos una discusión con ellas sobre cómo podemos ayudarlos a mejorar sus operaciones internas. [...] [En el desarrollo del proceso] comenzamos

⁴⁰⁸ «Informe de actividad 2019 de la Unidad de Referencia de Internet (IRU) de la Unión Europea», *Departamento de Seguridad Nacional (DSN) del Gobierno de España*, Disponible en: <https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-actividad-2019-unidad-referencia-internet-iru-union-europea> [Fecha de consulta: 01 de diciembre de 2023].

⁴⁰⁹ EUROPOL EU IRU OFFICIAL (2020): «A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit/Entrevistado por A. Amarasingam», *Ibidem*.

⁴¹⁰ Por la relevancia, la escasez de información relativa a la materia y por la riqueza de datos aportados en la entrevista referenciada en el pie de página inmediato anterior, se adjunta la entrevista completa. Véase Índice: ANEXOS. Anexo N.º 03: *Entrevista con un funcionario de la Unidad de Referencia de Internet de la UE de Europol [versión original y traducción al castellano]*.

detectando un nuevo archivo multimedia que una organización terrorista designada coloca en Internet y, siempre que estamos en condiciones de detectar y recopilar este contenido, recopilamos las URL y marcamos las URL de la publicación específica en las redes sociales. Otra forma en que los ayudamos [a las empresas de tecnología] es compartiendo algunas de nuestras experiencias, digamos, recopilando imágenes, logotipos o marcadores que utilizan organizaciones terroristas designadas. Compartimos este tipo de paquetes con ellos para ayudarlos a comprender cómo las organizaciones terroristas utilizan la marca para hacerse visibles y difundir su mensaje a audiencias más amplias. [...] [El cambio de paradigma de la empresas en relación con la libertad de expresión] no fue solo un cambio en la comprensión de las empresas de redes sociales, sino que fue un cambio en la comprensión de toda la comunidad internacional que analiza este tema específico de que no podemos permitir que las organizaciones terroristas exploten las redes sociales de acceso público y a proveedores de servicios en línea para promover su mensaje, planificar sus operaciones y llegar a las personas con fines de contratación y financiación. [Con esta nueva comprensión] hemos conseguido al menos el objetivo principal de restringir el acceso público a este tipo de contenidos. Cada vez es más difícil para el usuario promedio tropezar con contenido terrorista mientras navega diariamente por Internet. [...] [No obstante] el contenido terrorista, por supuesto, sigue siendo accesible en Internet. Nunca dijimos que nuestro trabajo sea limpiar Internet de contenido terrorista, pero nuestro trabajo es tratar de identificar quién está detrás de eso, atribuir los delitos terroristas a quienes están detrás de las pantallas y también proteger al público en general.»⁴¹¹

El contenido terrorista que tenga una ‘marca’, es decir que sea atribuible al aparato comunicativo ‘oficial’ de una organización, y no a un simpatizante aislado (*fanboys*) es para el EU IRU el contenido que realmente posee relevancia. A tenor de este tema, el especialista indica:

«[...] Siempre que tenga una marca, es parte de nuestra preocupación, pero por supuesto hacemos una distinción clara porque no se puede comparar una declaración oficial o una pieza de propaganda de la misma manera con una pancarta o algo producido por un *fanboy*, que no que relacionado con los medios de comunicación yihadistas. [...] [La respuesta a que preocupación] consideramos que es un esfuerzo conjunto que deben realizar otras partes interesadas, otros participantes en este trabajo contra el contenido terrorista. Por eso, también colaboramos con los investigadores. Hemos creado una red de asesores. Intentamos compartir nuestra experiencia, pero también integrar los resultados de la investigación de estos. [...] [Las] discusiones sobre cómo manejamos el contenido generado por seguidores es un tema crítico porque vemos que a veces el contenido producido solo por fanáticos puede aparecer en los titulares, puede reproducirse, lo que distorsiona la evaluación de la amenaza terrorista.»⁴¹²

EU IRU ayuda a crear conciencia sobre el modo en que se emplea el material terrorista en Internet que se utiliza con una finalidad informativa, institucional, académica, etc., es decir, ninguna finalidad delictiva. Para EU IRU, existe en estas acciones un riesgo de publicitar la marca del grupo terrorista.

«[El material yihadista] puede ser reproducido por personas que sin darse cuenta quieren informar sobre este contenido, pero al mismo tiempo ayudan a amplificarlo. Entonces, trabajamos en conjunto con instituciones, investigadores, etc., para generar conciencia sobre estos temas. Por ejemplo, cuando vemos que algunos periodistas o investigadores utilizan los mismos *hashtags* [creados por medios yihadistas para promocionar su contenido] o parte de un videoclip terrorista para informar sobre el terrorismo, podemos verlo como problemático porque al mismo tiempo, reproduces o difundes este mensaje. El punto aquí es que no debe circular contenido sin editar o contenido que publicite la marca de la organización terrorista. La mayoría de los profesionales adoptan un enfoque matizado, pero no siempre es así. Una vez más, contamos con una red ampliada de partes interesadas; Trabajamos con instituciones europeas, con la Red Europea de Comunicación Estratégica (ESCN), con la Red de Concientización sobre la Radicalización

⁴¹¹ EUROPOL EU IRU OFFICIAL (2020), opus cit.

⁴¹² *Ibidem*.

(RAN), con la red global de investigación creada por el Foro Global de Internet para Contrarrestar el Terrorismo (GIFCT).»⁴¹³

EU IRU de Europol identifica que ha habido una traslación del contenido yihadista de Internet de unas empresas hacia otras. La unidad EU IRU comenzó sus funciones en el año 2015 rastreando contenido yihadista en Internet. En ese entonces el grueso del material yihadista se encontraba alojado en las plataformas de *Facebook* y *Twitter* (actual X). Habiendo trabajado muy cerca, desde un inicio, con estas empresas y habiendo colaborado estas empresas en la eliminación de contenido terrorista, así como en la pronta identificación para la prevención de nuevas publicaciones, los grupos terroristas se vieron forzados a buscar nuevas plataformas de tecnología para publicar y difundir su información (videos, audios, escritos, canciones, etc.) en Internet. En principio los grupos terroristas migraron a *Telegram*. *Telegram* entonces se convirtió en el epicentro de la propaganda terrorista. Por medio de esta plataforma se compartieron los discursos de los líderes, avisos de martirio, ataques y comunicados de prensa semanales. Los investigadores académicos que, hace apenas una década o dos, tenían que “esperar a que los grupos terroristas publicaran sus vídeos granulados desde escondites en las montañas para tener una idea de lo que querían comunicar al mundo, ahora tenían en sus teléfonos inteligentes acceso a decenas de miles de publicaciones.”⁴¹⁴ Tras la gran intervención, en el año 2019, de los contenidos terroristas alojados en *Telegram*, las organizaciones terroristas establecieron una nueva migración⁴¹⁵ y comenzaron a utilizar *TamTam*⁴¹⁶ y *Hoop Messenger*⁴¹⁷. Sobre aquellos hechos de migración de contenidos online del terrorismo, el especialista recuerda:

«[...] comenzamos nuestras observaciones rastreando el contenido. Entonces, cuando se mudaron a Telegram, intentamos comunicarnos con Telegram y explicar la situación. Comenzamos a señalar contenido terrorista en Telegram y gradualmente establecimos un canal de comunicación y cooperación con Telegram. Las empresas de tecnología, cuando crean su propio negocio, no piensan en la explotación de su plataforma por parte de terroristas. Entonces, para muchas empresas, no solo para Telegram, el primer paso es crear conciencia sobre lo que sucede en su plataforma y luego comenzar a generar confianza con ellas. Esto es importante y por eso destacamos la importancia de la cooperación voluntaria, la importancia de la asociación público-privada. Si soy honesto, de algunos de los proveedores de servicios en línea con los que intentamos interactuar, su primera reacción es ¿Por qué una agencia policial me pide que revise este tipo de contenido?, ¿Qué hay detrás de eso?, ¿Vienes con un mandato legal?, ¿Vas a pedir

⁴¹³ *Ibidem*.

⁴¹⁴ «Telegram Deplatforming ISIS Has Given Them Something to Fight For», *VICE News*. Disponible en: <https://www.vice.com/en/article/vb55bd/telegram-deplatforming-isis-has-given-them-something-to-fight-for> [Fecha de consulta: 02 de diciembre de 2023].

⁴¹⁵ *Ibidem*.

⁴¹⁶ TamTam es una aplicación de mensajería instantánea con un cifrado seguro de *chats*, canales, videollamadas y servicios de geolocalización. El creador de TamTam es una empresa rusa de Internet llamada Mail.Ru Group y, dentro de esta empresa, la aplicación de mensajería ha sido desarrollado por su proveedor de servicios de redes sociales, Odnoklassniki. La aplicación comenzó a estar disponible a principios de 2017. El uso de esta aplicación por parte del yihadismo se puede resumir en las siguientes palabras de Pieter Van Ostacyen, miembro de la junta directiva del Centro Internacional para la Lucha contra el Terrorismo: “Hubo una actividad extrema en TamTam. Podrías irte a la cama conectado a 20 canales y despertarte con más de 1.000 notificaciones en TamTam”. Véase: «The Russian Social Network Letting ISIS Back Online», *VICE News*. Disponible en: <https://www.vice.com/en/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app> [Fecha de consulta: 02 de diciembre de 2023].

⁴¹⁷ Hoop Messenger es una aplicación de mensajería desarrollada por Magnificus Software (Vancouver, British Columbia, Canadá) en el año 2014. Permite a los usuarios realizar llamadas cifradas sin que terceros escuchen. Se puede utilizar para llamadas de voz, enviar mensajes y navegar por la web sin necesidad de una VPN externa, dado que Hoop Messenger tiene un navegador VPN integrado. Cuenta con una base de datos segura que protege llamadas y videos por cifrado de extremo a extremo. También posee muchos canales públicos que permiten acceder a una comunidad de bloggers, redactores de contenido, activistas, fotógrafos, etc., y recibir de sus canales las últimas actualizaciones sobre el tema escogido.

más información? Nosotros [Europol] no tenemos ningún poder de ejecución allí. Nuestro mandato legal es marcar el contenido y luego trabajar junto con ellas [las empresas de redes sociales] para crear conciencia. Entonces, es su propia decisión. Así también funcionó con Telegram. [...] Esto era parte de nuestro procedimiento estándar al relacionarnos con proveedores de servicios en línea. Ya habíamos realizado un par de, digamos, acciones junto con Telegram en el pasado [se refiere al año 2018]. Cubrimos una gran cantidad de proveedores de servicios en línea, no solo Telegram. Pero en algún momento del año pasado, nos tomamos un tiempo para analizar específicamente Telegram. Hicimos una acción conjunta [RAD del 21 y 22 de noviembre de 2019] y luego comenzamos a construir a partir de ese momento para tratar de trabajar más estrechamente para mapear la red de diseminadores centrales, por así decirlo, propagandistas cuyo negocio principal es difundir este tipo de contenido. Y esta cooperación culminó con este tipo de acción, pero al mismo tiempo, hemos estado trabajando junto con las Fuerzas del orden en los Estados Miembros para interrumpir las operaciones en Internet del Estado Islámico. En el pasado, hicimos algún trabajo de investigación y, junto con los fiscales, logramos detener algunos de los activos web (por ejemplo, servidores) que los propagandistas del Estado Islámico estaban usando para almacenar contenido y comunicarse. [...] [Se desarrollaron acciones conjuntas entre] los fiscales, los investigadores de los Estados Miembros que trabajan en la parte de investigación y luego también los especialistas en contenido, los especialistas en derivaciones que trabajan con Telegram, y otras plataformas para derivar este tipo de contenido. Esta fue una acción planificada y sabíamos que, si salía bien, sacudiría a la comunidad de propagandistas yihadistas en Telegram. Y al interrumpir sus operaciones en Telegram, se crean nuevas oportunidades [para quienes trabajan en contraterrorismo]. Quiero decir, no fue tan difícil adivinar qué intentarían a continuación. Por supuesto, no lo sabemos todo, pero ya desde 2018 hubo algunos indicios de que estaban dispuestos a experimentar con determinadas plataformas. No fue una gran sorpresa que intentaran volver atrás y utilizar algunas de estas plataformas [con las que habían trabajado previamente: *Facebook* y *Twitter*]. Por supuesto, experimentaron con algunas plataformas nuevas, pero esto crea muchas oportunidades [para quienes trabajan en contraterrorismo]. En primer lugar, esto crea muchas perturbaciones. Luego tiene un impacto en la marca, porque nadie está seguro de quién está creando los nuevos canales, los nuevos canales Nashir, los nuevos canales Amaq, en cada nueva plataforma. ¿Cuál es el mensaje? Vemos ahora muchos mensajes que advierten a los protagonistas o simpatizantes de usar esta u otra plataforma, o usar o seguir este u otro medio de comunicación. Por lo tanto, hay un claro impacto en la marca y también existe la oportunidad de crear nuevas pistas de investigación. [...] lo que estoy diciendo aquí es que en el pasado trabajamos tanto en los aspectos de investigación/atribución como en los de remisión. [...] Entonces, este no es el final de la historia. Este es el comienzo de la historia y es por eso por lo que realmente queremos involucrarnos con la comunidad internacional, para unir todos nuestros esfuerzos para trabajar tanto en la prevención como en la atribución. Al dismantelar las redes yihadistas en Internet, se contribuye a la prevención.»⁴¹⁸

En este proceso de investigación, atribución y remisión del material yihadista en Internet, EU IRU destaca que es fundamental el compromiso tripartito de los EEMM y el sector privado. Cada Estado Miembro, así como cada empresa de tecnología en Internet posee un rol relevante en la lucha contra el terrorismo online. En los últimos años, la unidad ha observado una evolución positiva por parte de las empresas privadas a colaborar con la UE y con Europol en este ámbito.

«[...] ahora existe un entendimiento entre las empresas de redes sociales de que no deberían tolerar este tipo de explotación. Una vez más, esto depende de la plataforma y de su relación con los investigadores y fiscales de los Estados Miembros. Vemos que algunas plataformas están más dispuestas que otras a compartir información adicional. Esto no tiene nada que ver con la libertad de expresión. Por supuesto, estamos a favor de la protección de la libertad de expresión y los derechos fundamentales y los derechos digitales de los ciudadanos, pero nuestro enfoque es muy específico. Y vemos que las empresas empiezan a ver esto como otro tipo de delito en torno al cual ya han estado trabajando con las autoridades, como el

⁴¹⁸ EUROPOL EU IRU OFFICIAL (2020), opus cit.

fraude bancario o la explotación sexual infantil. Están dispuestos a compartir más datos porque ven un beneficio en interrumpir estas redes y llevar a estas personas ante la justicia.»⁴¹⁹

De las 16.^a Jornadas de Acción de Referencia conjunta celebradas en La Haya entre el 21 y 22 de noviembre de 2019, la EU IRU obtuvo suficiente información sobre actos criminales en Internet para que se llevara a cabo la operación de noviembre de 2019. Esta operación “fue dirigida por el juez de investigación antiterrorista belga y la Fiscalía Federal belga, junto con la Policía Judicial Federal belga de Flandes Oriental” y, entre diversas actuaciones policiales, se concreta “un arresto en España de un individuo sospechoso de ser parte de los principales difusores de propaganda terrorista del Estado Islámico”⁴²⁰ en Internet. Para EU IRU de Europol:

«Esto está relacionado con el trabajo operativo. [...] Los Estados Miembros estaban trabajando junto con nosotros para confiscar algunos de los activos y crear algunas pistas de investigación. Esta fase de la operación (me refiero a la parte de investigación, no a la de remisión) fue dirigida por las autoridades judiciales belgas, y los colegas belgas y españoles querían presentar un mensaje contundente de que éste es el camino por seguir. Todos nos unimos y trabajamos juntos para atribuir los delitos terroristas a los perpetradores.»⁴²¹

Para llegar a la fase operativa, la EU IRU desarrolla una ardua tarea de investigación que implica el conocimiento no solo de la promoción de la propaganda en Internet, sino también de todas las actividades posteriores a una publicación yihadista. La unidad no solo realiza un monitoreo en la red de contenido terrorista, sino que comprende el mensaje. Por ello no se centra en el material aislado, sino en la marca, las campañas y la estrategia de la organización terrorista.

«[En la comunicación del Estado Islámico] hay diferentes capas de la estructura [...] para producir y difundir contenidos. En el apogeo de su actividad, han diseñado a Amaq como una agencia de noticias independiente para informar sobre la evolución sobre el terreno en tiempo real. Al mismo tiempo, contaban con los medios de comunicación avalados oficialmente. Luego hubo otra capa de medios de comunicación de apoyo [...] para apoyar el trabajo del Estado Islámico, pero, al mismo tiempo produjeron su propio contenido terrorista y lo difundieron. Y luego, una tercera capa compuesta por simpatizantes que estaban dispuestos a crear contenido generado por sus seguidores y difundirlo. [...] le damos diferentes pesos a estas capas. [...] Además, en el pico de su actividad, solían tener una campaña muy sofisticada en Internet que comenzaba con el envío de *teasers* sobre nuevos lanzamientos, como las revistas que iban a sacar. Esto fue lo que pensábamos que era la “fase de siembra”. Luego estuvo la “fase de lanzamiento” y luego tuvieron la “fase de eco” en la que publicitaron contenido en grandes volúmenes. Esta fue una campaña sofisticada de su parte en lo que respecta a comunicaciones estratégicas, y este también ha sido el objetivo de nuestras operaciones, [...] trabajando junto con los Estados Miembros y las Fuerzas del orden, se obtiene información valiosa, y creo que, en los últimos años, los Estados Miembros, las Fuerzas del orden y los servicios judiciales han logrado desarticular parte de esta red y traer a estas personas a la justicia. Este es un esfuerzo continuo, un trabajo en progreso. [...] para nosotros es importante seguir trabajando con las autoridades y los Estados Miembros. Son responsables de las investigaciones y de tratar con quienes se unen a la organización terrorista en su esfuerzo por propagar sus narrativas. También queremos compartir nuestra experiencia con otras instituciones. Mencioné, por ejemplo, la Red de Sensibilización sobre la Radicalización porque la prevención es igualmente importante. Somos un centro antiterrorista y nos ocupamos del contrterrorismo, pero creo que nuestra experiencia es valiosa para otros que trabajan en el ámbito de la prevención. Por eso, tratamos de involucrarnos, tratamos de compartir nuestra experiencia y nuestro conocimiento, y esperamos que se aborden las causas

⁴¹⁹ *Ibidem*.

⁴²⁰ «EU law enforcement and judicial authorities join forces to disrupt terrorist propaganda online», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online> [Fecha de consulta: 02 de diciembre de 2023].

⁴²¹ EUROPOL EU IRU OFFICIAL (2020), opus cit.

profundas del terrorismo y que se realice un trabajo preventivo para evitar que la gente recurra a este tipo de actividad.»⁴²²

La EU IRU no solo actúa como una unidad de monitoreo e investigación de Internet, sino que promueve una vertiente preventiva a fin de evitar que las publicaciones yihadistas y su material discursivo promuevan más actos de violencia terrorista. La línea de la prevención que anteriormente habíamos observado en el desarrollo normativo de la Unión Europea y del Consejo, se mantiene presente en las medidas adoptadas de carácter operativo e interinstitucional. La Política Criminal de la Unión Europea con relación al terrorismo yihadista parece seguir la pauta de la prevención en todos aquellos ámbitos en los que puede tener algún tipo de injerencia. En el marco de las acciones operativas tendientes a la represión del terrorismo en la red, la EU está estrechando lazos de cooperación con el sector privado como nunca lo ha hecho en toda su historia.

En el contexto de la asociación público-privada que promueve la UE para prevenir la radicalización en línea y salvaguardar los derechos fundamentales, entre el Centro Europeo Contra el Terrorismo (ECTC) de Europol y la empresa de tecnología *TikTok*⁴²³ se llevó a cabo un nuevo RAD⁴²⁴.

Este RAD, que tuvo lugar el 28 de septiembre de 2023, fue desarrollado como iniciativa conjunta entre España y la EU IRU, y contó con la colaboración de la plataforma *TikTok* y de autoridades policiales de diez Estados⁴²⁵ participantes. Este dispositivo impulsado por España contó internamente con el apoyo del Centro de Inteligencia contra el Terrorismo y Crimen Organizado (CITCO) del Ministerio del Interior, quien fue el responsable de coordinar a la Policía Nacional, Guardia Civil, Mossos d'Esquadra y Ertzaintza. La actuación de los investigadores de estas Cuerpos y Fuerzas de Seguridad del Estado español se tradujeron en el aporte cuantificable de más del 50% de las publicaciones sospechosas comunicadas a *TikTok*.⁴²⁶

Todos los asistentes, junto con la Unidad de Referencia de Internet de la Unión Europea (EU IRU), realizaron un ejercicio para detectar material que glorificaba ataques terroristas pasados o a perpetradores terroristas.

Como parte del ejercicio conjunto, se evaluaron unos 2.145 contenidos y se señalaron a *TikTok* para su revisión voluntaria según sus términos de servicio⁴²⁷. Entre los contenidos referidos se

⁴²² *Ibidem*.

⁴²³ *TikTok* es una red social de origen chino que permite compartir videos. Es propiedad de la empresa china ByteDance, y es la versión internacional de la red social Douyin. La plataforma se utiliza para hacer una variedad de videos en formato corto y vertical, cuya duración varía entre 1 segundo y 10 minutos. Estos videos no tienen un plazo determinado de reproducción, por lo tanto cuando acaban vuelven a empezar otra vez, en un bucle infinito. *TikTok* y Douyin tienen una interfaz de usuario muy similar pero no tienen acceso al contenido del otro. Cada uno de sus servidores está basado en el mercado donde la aplicación respectiva está disponible y están sujetos a la normativa donde opera.

⁴²⁴ «Europol and TikTok collaborate to bolster efforts against terrorist content», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-tiktok-collaborate-to-bolster-efforts-against-terrorist-content#:~:text=On%2028%20September%2C%20a%20large,and%20violent%20extremist%20content%20online>. [Fecha de consulta: 02 de diciembre de 2023].

⁴²⁵ Chequia, Dinamarca, Francia, Alemania, Hungría, Irlanda, Malta, Portugal, Suecia y Reino Unido, *Ibidem*.

⁴²⁶ «España y Europol lideran la retirada de más de 2.000 contenidos terroristas de *TikTok*», *Ministerio del Interior*, 5 octubre 2023. Disponible en: <https://www.interior.gob.es/opencms/en/detail-pages/article/Espana-y-Europol-lideran-la-retirada-de-mas-de-2.000-contenidos-terroristas-de-TikTok/> [Fecha de consulta: 02 de diciembre de 2023].

⁴²⁷ «*TikTok publica periódicamente estadísticas de eliminación de contenido de extremismo violento en sus informes trimestrales de transparencia. El último informe muestra que TikTok eliminó de forma proactiva el 95% del contenido de extremismo violento.*»

encontraban elementos vinculados al yihadismo y al extremismo violento de derecha y al terrorismo, como vídeos y memes.

Como consecuencia de esta colaboración voluntaria con la UE, algunas compañías de tecnología han comenzado a desarrollar iniciativas propias a fin de aplicarlas de forma interna a sus protocolos de actuación empresarial. Tal es el caso de *Facebook* quien desarrolló una "lista negra" interna la cual estaría conformada por más de 4.000 personalidades y grupos. La lista engloba a aquellas personas o movimientos que tienen vetado el uso de sus plataformas por estar vinculados al terrorismo o con otras formas de acción violenta. Entre los aspectos que contempla se encuentra aquellos relacionados con delitos de odio, crimen en todas sus formas, terrorismo, movimientos paramilitares y grupos violentos ajenos o enemigos de Estados. Sí bien naturalmente esto es parte de las políticas de uso de la plataforma de Facebook, y su aplicabilidad es global, es decir, más allá de las fronteras de la Unión Europea, no puede dejar de considerarse el hecho de que estas iniciativas de orden privado responden en gran medida a las informaciones suministradas por EU IRU sobre el uso desvirtuado y criminal que se hace en ocasiones de la tecnología que crean las empresas.

Lo que es indudable es el hecho de que las empresas están comenzando a pensar la seguridad bajo otros términos. Ello significa, más allá de la seguridad informática. Las grandes compañías de tecnología tradicionalmente han pensado en la seguridad como algo vinculado de forma exclusiva y directa a sus intereses empresariales, a sus activos tecnológicos (información digital protegida, desarrollo I+D y patentes, etc.). En los últimos años, las compañías de tecnología están adquiriendo una conciencia acerca de cómo sus plataformas pueden ser utilizadas de forma criminal, y por tanto, su concepto de seguridad está cambiando, y adquiriendo realmente una dimensión global, no solo empresarial. Tal es la relevancia de este nuevo enfoque que como ha reconocido Brian Fishman⁴²⁸, gestor de Políticas Contraterroristas de Facebook, la empresa actualmente posee un equipo de 150 especialistas que trabajan en 30 lenguas y se encargan de revisar el contenido.

No obstante, a todos los esfuerzos realizados,

«*Facebook* ha recibido críticas por no hacer lo suficiente para monitorear su sitio y eliminar contenido publicado por grupos extremistas. En mayo, Theresa May, la primera ministra del Reino Unido, anunció que buscará que las empresas de Internet —entre ellas *Facebook*— hagan más por monitorear y detener a estos grupos.»⁴²⁹

Berger J. M., miembro del *International Centre for Counter-Terrorism* (ICCT) en La Haya, dijo que gran parte del desafío para empresas como *Facebook* es averiguar qué califica como terrorismo. Sin embargo, indicó que tenía la esperanza de que la nueva tecnología de inteligencia artificial pudiera usarse para contrarrestar cualquier forma de extremismo que violara los términos de uso de la empresa, aunque por el momento se enfocará de manera restringida y/o se desconociera su enfoque. Ante estas declaraciones *Facebook* expresó que "al igual que otras

Véase: «Europol and TikTok collaborate to bolster efforts against terrorist content», *CT Insight*, 5 octubre 2023. Disponible en: <https://ctinsight.net/europol-and-tiktok-collaborate-to-bolster-efforts-against-terrorist-content/> [Fecha de consulta: 02 de diciembre de 2023].

⁴²⁸ «Brian Fishman», *New America*. Disponible en: <https://www.newamerica.org/our-people/brian-fishman/> [Fecha de consulta: 02 de diciembre de 2023].

⁴²⁹ «Facebook usará inteligencia artificial para combatir las publicaciones extremistas», *New York Times*, edición online de 19 de junio de 2017. Disponible en: <https://www.nytimes.com/es/2017/06/19/espanol/facebook-extremismo-inteligencia-artificial.html> [Fecha de consulta: 03 de diciembre de 2023].

compañías tecnológicas, no hemos compartido la lista para limitar el riesgo legal, evitar los riesgos de seguridad y minimizar las oportunidades para que los grupos eludan las reglas.”⁴³⁰

Aun cuando *Facebook* mantiene su lista negra en reserva, la empresa ha detallado el modo en que cataloga las publicaciones de los usuarios que ingresan a la misma. *Facebook* establece el foco en la peligrosidad que implica la publicación y determina tres rangos de clasificación.

El rango primero, el de mayor peligrosidad, involucra comentarios positivos o posturas defensivas de personas o grupos considerados violentos, aun cuando los hechos o acciones que se alaben no sean necesariamente violentos. Esta categoría se reserva especialmente para los grupos terroristas. Se encuentran categorizados en este rango cerca de 500 organizaciones criminales, y más de 250 supremacistas blancos.

En un segundo nivel, se categoriza a los usuarios que expresan su aprobación por actividades no violentas de los grupos del primer rango, pero no dan un apoyo sustancial al grupo en cuestión. *Facebook* no ha definido explícitamente a qué se refiere con “apoyo sustancial”. No obstante, según la teoría, podría tratarse de un tipo de apoyo que implica antipatía hacia los occidentales y simpatía hacia el terrorismo. Según Moyano y Trujillo “estas actitudes podrían estar sirviendo como una base de apoyo sustancial que los terroristas pueden estar utilizando y que sin duda pueden instrumentalizar.”⁴³¹

Finalmente, el tercer y último rango se compone por grupos que no ejercen la violencia, pero sí son susceptibles de radicalizarse y volverse violentos. Se caracterizan por utilizar con frecuencia el discurso de odio.

Los esfuerzos hechos a iniciativa privada como el realizado por Facebook y por otras empresas del sector, parecen ser insuficientes para implementar mecanismos estandarizados que permitan reprimir el crimen de terrorismo online con la eficacia y rapidez necesaria. La Unión Europea exige aún más esfuerzos en esta materia a fin de poder alcanzar un mayor índice de satisfacción en el logro de este objetivo. El 9 de diciembre de 2020, el Parlamento Europeo y los Estados Miembros de la UE lograron:

«[...] un acuerdo político para imponer a las plataformas digitales como *Facebook*, *YouTube* o *Twitter* [actual X] la obligación de retirar en un máximo de una hora, y a petición de los Estados Miembros, contenidos terroristas que estén siendo difundidos a través de sus redes en Internet.»⁴³²

Ello significa que las compañías de tecnología en Internet tendrán un plazo máximo de 60 minutos para cumplir con la orden. Los EEMM serán los responsables en cada caso particular de asegurarse que las plataformas siguen las indicaciones para su cumplimiento, y de establecer, en caso de incumplimiento, el marco de sanciones internas aplicable. “El acuerdo avanza también en materia de cooperación y apunta una coordinación reforzada entre las autoridades nacionales y Europol para un mejor seguimiento de las órdenes de retirada de contenidos en toda la Unión Europea.”⁴³³

⁴³⁰ «Así es la lista negra de Facebook para individuos y organizaciones peligrosas», *Escudo Digital*, edición online de 3 de octubre de 2021. Disponible en: https://www.escudodigital.com/sociedad/seguridad-y-consumo/asi-es-la-lista-negra-de-facebook-para-individuos-y-organizaciones-peligrosas_34556_102.html [Fecha de consulta: 03 de diciembre de 2023].

⁴³¹ MOYANO PACHECO, Manuel/TRUJILLO MENDOZA, Humberto Manuel (2013): *Radicalización Islamista y Terrorismo. Claves psicosociales*. Granada: UGR-MADOC; p. 146.

⁴³² «Facebook, Twitter o YouTube deberán retirar contenidos terroristas en una hora en la Unión Europea», *Escudo Digital*, edición online de 10 de Diciembre de 2020. Disponible en: https://www.escudodigital.com/defensa/facebook-twitter-o-youtube-deberan-retirar-contenidos-terroristas-en-una-hora-en-la-union-europea_22127_102.html [Fecha de consulta: 03 de diciembre de 2023].

⁴³³ *Ibidem*.

Esta iniciativa fue propuesta por la Comisión Europea en el año 2018, pero no se llegó a un acuerdo en ese entonces por diferencias entre gobiernos de los EEMM, y eurodiputados entre sí acerca de su aplicación y de su protección de los derechos fundamentales. Sin embargo, tras los atentados en Francia (Atentado en Notre-Dame, Niza, 2020) y Austria (Atentados en Viena, 2020) la negociación prosperó y se consolidó el acuerdo.

A partir de este acuerdo, las reglas se aplicarán a todas las empresas de Internet que ofrezcan servicios dentro de la Unión Europea, con independencia de dónde se ubique la sede legal de la plataforma o de cuál sea el tamaño de la compañía. Por medio de este acuerdo, las compañías también estarán obligadas a presentar informes anuales para informar con transparencia sobre las acciones emprendidas en sus empresas.⁴³⁴

En el año 2022, la Unión Europea da un gran salto cualitativo en el ámbito de la cooperación al introducir la Ley de Servicios Digitales⁴³⁵ (DSA)⁴³⁶, un reglamento que podrá ser considerado histórico por los cambios normativos que introduce a fin de regular la relación entre el sector público y el sector privado. Sí bien no es de aplicación exclusiva para el delito de terrorismo en Internet, sí que supone un mayor control y restricción sobre este tipo de uso.

La Ley de Servicios Digitales (DSA) se encuentra dentro de un Paquete de Ley de Servicios Digitales⁴³⁷ y exige a las empresas tecnológicas consideradas “grandes plataformas digitales”⁴³⁸ el cumplimiento de normas más estrictas para el desarrollo de sus funciones en la región europea. La Ley de Servicios Digitales (DSA) está orientada a fomentar la transparencia, a reducir la desinformación (*fake news*) y lo contenidos ilegales en Internet. La pretensión de la DSA es promover la máxima seguridad de la Europa digital.

La Unión Europea identifica como servicios digitales a una gran variedad de servicios en línea, desde sitios web hasta servicios de infraestructura de Internet y plataformas de comunicación. Por medio de esta ley las empresas de servicios digitales que operan en la UE pasarán de la colaboración voluntaria al cumplimiento de una legislación obligatoria.

Conforme a la Ley de Servicios Digitales (DSA), las empresas señaladas deberán de ahora en más cumplir con los siguientes requisitos para poder operar en el mercado europeo:

⁴³⁴ El acuerdo no persigue la difusión de contenido realizada bajo fines educativos, periodísticos, artísticos o de investigación, así también como los archivos difundidos cuya finalidad sea crear conciencia contra el delito de terrorismo.

⁴³⁵ REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales). La DSA se publicó en el Diario Oficial el 27 de octubre de 2022 y entró en vigor el 16 de noviembre de 2022; no obstante, su aplicación total y directa en toda la UE será a partir del 17 de febrero de 2024.

⁴³⁶ DSA por sus siglas en inglés (*Digital Service Act*, -Ley de Servicios Digitales-).

⁴³⁷ El Paquete de Ley de Servicios Digitales integra dos leyes: la Ley de Servicios Digitales (DSA) y la Ley del Mercado Digital (DMA). Está última regulará solo las grandes empresas en términos estrictamente comerciales. Aquella que resulta de nuestro interés es la Ley de Servicios Digitales (DSA), cuya aplicación tiene como objeto crear para Europa un espacio digital más seguro en el que se protejan los Derechos fundamentales de todos los usuarios de servicios digitales. Véase: «Paquete de la Ley de Servicios Digitales», Comisión Europea, 25 de septiembre de 2023. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package> [Fecha de consulta: 03 de diciembre de 2023].

⁴³⁸ La Comisión Europea ha realizado una primer lista de 19 empresas consideradas muy grandes. Tal calificación se debe a que son empresas que poseen unos 45 millones de usuarios activos mensuales. De las 19 empresas, 17 son plataformas en línea, y entre estas se encuentra *Alibaba*, *AliExpress*, *Amazon Store*, *Apple AppStore*, *Booking.com*, *Facebook*, *Google Play*, *Google Maps*, *Google Shopping*, *Instagram*, *LinkedIn*, *Pinterest*, *Snapchat*, *TikTok*, *Twitter*, *Wikipedia*, *YouTube* y *Zalando*. Las 2 empresas restantes cumplen el mismo criterio en cuanto al número de usuarios activos mensuales, pero son catalogados como motores de búsqueda en Internet. Ellos son *Bing* y *Google Search*. Véase: «La Unión Europea impondrá controles más estrictos a las grandes plataformas digitales», *Euronews*, edición online de 25 de abril de 2023. Disponible en: <https://es.euronews.com/my-europe/2023/04/25/la-ue-impondra-controles-mas-estrictos-a-las-grandes-plataformas-digitales> [Fecha de consulta: 03 de diciembre de 2023].

1. Etiquetar el contenido creado por Inteligencia Artificial (AI) y que encuentre publicado en Internet. La finalidad es luchar contra la desinformación.⁴³⁹
2. Las empresas deben poner a disposición de los usuarios una herramienta automatizada, con condiciones de uso fácilmente comprensibles, para señalar dentro de sus plataformas los contenidos ilegales. La finalidad es que el ciudadano asuma un rol colaborativo en el ámbito de la seguridad de Internet sobre los contenidos ilegales.
3. Las plataformas deberán crear un algoritmo de Inteligencia Artificial (AI) que les permita identificar, referenciar a Europol y eliminar contenido ilegal. La finalidad de ello es restringir el flujo de contenido ilícito.
4. Las plataformas deberán crear un algoritmo que le brinde al usuario un flujo alternativo de contenido, que no esté basado en los algoritmos de recomendación habitual según la búsqueda del usuario. El objetivo es hacer salir al usuario de “esa nube informativa”.⁴⁴⁰ La finalidad de este punto está orientada a evitar la formación de *echo chambers*⁴⁴¹, basadas en supuestos intereses de los usuarios.
5. Las plataformas tendrán que permitir que expertos del recién creado Centro Europeo para la Transparencia Algorítmica (ECAT)⁴⁴², una nueva agencia de la UE, evalúen si su algoritmo cumple las distintas obligaciones requeridas.
6. Las empresas deben suministrar a la UE un informe con carácter anual en donde se evalúen los riesgos y amenazas a sus plataformas de servicios de Internet.

Los Estados Miembros de la Unión Europea, por su parte, tendrán la obligación de nombrar coordinadores de servicios digitales a más tardar el 17 de febrero de 2024, fecha de implementación total de la DSA.

Las nuevas prácticas facilitarán la persecución de los contenidos terroristas y extremistas en Internet. Las medidas que deben cumplir las grandes empresas implican materializar en sus plataformas nuevas funcionalidades (por medio de botones automatizados) que les permita a usuarios y desarrolladores señalar fácilmente contenido criminal alojado en sus plataformas. Además, los resultados de búsqueda se basarán únicamente en las palabras que el usuario escriba en el buscador cada vez que ingrese a la plataforma, de tal manera que no se personalizarán en función de la actividad o interés anterior o presumible del usuario. Esto ayudará a disminuir el vigor de las *echo chambers*. En el proceso propagandístico o de radicalización del yihadismo habíamos comentado previamente que es determinante la existencia de las *echo chambers* para el cumplimiento de los objetivos de la promoción y difusión del terrorismo yihadista. El

⁴³⁹ Herramientas como *ChatGPT* son capaces de crear contenidos muy realistas en cuestión de segundos, aunque estos textos puedan estar cargados de información falsa. Lo mismo ocurre con otras herramientas de IA que pueden crear fotos, vídeos y audios que nunca han ocurrido en la realidad.

⁴⁴⁰ «Europa cambia las reglas de juego para Google, Facebook y TikTok: una inédita ley ya está en vigor y así funciona», *Diario Clarín*, edición online de 25 de agosto de 2023. Disponible en: https://www.clarin.com/mundo/europa-cambia-reglas-juego-google-facebook-tiktok-inedita-ley-vigor-funciona_0_GcDzCUMMnN.html [Fecha de consulta: 04 de diciembre de 2023].

⁴⁴¹ La cámara de eco (*echo chamber*), es un fenómeno comunicativo que tiene lugar en las redes sociales mediante el cual los usuarios tienden a encontrar ideas que amplifican y refuerzan sus propias creencias.

⁴⁴² La Comisión está creando un Centro europeo para la Transparencia Algorítmica (ECAT, *European Centre for Algorithmic Transparency*) para apoyar su función supervisora con conocimientos multidisciplinares internos y externos. El ECAT brindará asistencia y controlará si el desarrollo de sistemas de algoritmos de las empresas está en consonancia con las obligaciones de gestión de riesgos que establece la Ley de Servicios Digitales para las plataformas y los motores de búsqueda. Véase: «European Centre for Algorithmic Transparency», *Comisión Europea*. Disponible en: https://algorithmic-transparency.ec.europa.eu/index_en [Fecha de consulta: 04 de diciembre de 2023].

software existente hasta la fecha recoge la navegación del usuario para ofrecerle contenido de características idénticas o similares. Ello genera una cámara de eco que refuerza los intereses e ideas del individuo. En un sujeto delictivo, cuyo interés es el terrorismo y su ideología se basa en la yihad violenta, la existencia de *echo chambers* en Internet supone a priori un agravamiento del problema porque fomenta una realidad sesgada. No obstante, la propia DSA contempla que estos sistemas de recomendación automatizados sean activados y desactivados por el propio usuario de acuerdo sus preferencias de uso de la propia plataforma.

La legislación entró en vigor el 16 de noviembre de 2022, y las grandes plataformas han contado con cuatro meses para cumplir todas las nuevas obligaciones de la DSA, que incluyó, entre todas las mencionadas, llevar a cabo y proporcionar a la Comisión su primera evaluación anual de riesgos. Aun así, las empresas de tecnología no solo incorporaron las normas requeridas, sino que comenzaron a implementar procesos internos para facilitar el cumplimiento de las mismas. *TikTok*, por ejemplo, es una de las primeras plataformas en implementar los cambios y ofrece a sus usuarios una opción de “Guía de categorías de denuncia de contenido ilegal” que contempla la existencia de una clasificación exhaustiva que permita identificar entre una variedad de opciones, cuál es el delito que el usuario observa ante sí y que desea reportar.⁴⁴³ Asimismo, la empresa china *ByteDance* (la empresa desarrolladora de *TikTok*) ha contratado un nuevo equipo de moderadores y expertos legales, que junto al equipo de moderación ya existente y al trabajo de sistemas automatizados de identificación de contenido, llevará a cabo la revisión de los videos denunciados por los usuarios.

Facebook aún no ha implementado los cambios en su plataforma, pero ha anticipado, según el presidente de Asuntos Globales de Meta, Nick Clegg, que la DSA es “una de las regulaciones de Internet más completas”, y afirma que adaptarán sus sistemas de procesos a las nuevos requisitos.⁴⁴⁴

Por su parte, de cara al cumplimiento de la DSA, *Instagram* ha modificado y establecido nuevas condiciones de uso de la plataforma, las cuales entraran en vigor el 12 de enero de 2024.⁴⁴⁵

El comisario europeo de Mercado Interior Thierry Breton, quien fuera el principal impulsor de la nueva ley, expresó en un vídeo publicado en Twitter:

«Todo lo que está prohibido en la vida real será prohibido en Internet. [...] Gracias a la Ley de Servicios Digitales, los ciudadanos y las empresas europeas se beneficiarán de un Internet más seguro. [...] A partir del 25 de agosto, las plataformas en línea y los motores de búsqueda con más de 45 millones de usuarios

⁴⁴³ Entre los delitos listados se encuentra (en el siguiente orden): Explotación sexual infantil, Delitos de terrorismo, Incitación ilegal al odio, Contenido relacionado con la delincuencia violenta u organizada, Violaciones ilegales de la intimidad, Intercambio de imágenes privadas o íntimas sin consentimiento, Bienes o servicios ilegales, Acoso o amenazas, Difamación, Delitos relacionados con los consumidores, Delitos relacionados con la información, Delitos financieros, Delitos contra la seguridad nacional, Otro contenido ilegal. Véase: «Cómo denunciar contenido ilegal», *TikTok*. Disponible en: <https://www.tiktok.com/legal/page/global/reporting-illegal-content/es> [Fecha de consulta: 04 de diciembre de 2023]. Nota adicional: la protección de los menores por parte de *TikTok* (el segmento etario de usuarios más numeroso que posee esta plataforma) no surgió a iniciativa propia, sino que responde a las advertencias previas de Bruselas. Véase: «Bruselas advierte a TikTok: se expone a multas o un veto temporal si no protege a los menores», *La Vanguardia*, 20 de enero de 2023. Disponible en: <https://www.lavanguardia.com/tecnologia/redes-sociales/20230120/8697009/bruselas-advier-te-tiktok-enfrenta-sanciones-e-prohibicion-protecte-menores-pmv.html> [Fecha de consulta: 04 de diciembre de 2023].

⁴⁴⁴ «Facebook e Instagram permitirán que veas las historias y los reels de forma cronológica», *ABC*, edición online de 22 de agosto de 2023. Disponible en: <https://www.abc.es/tecnologia/redes/facebook-instagram-permitiran-veas-historias-reels-forma-20230822171515-nt.html> [Fecha de consulta: 04 de diciembre de 2023].

⁴⁴⁵ «Condiciones de uso de Instagram», *Instagram*. Disponible en: https://help.instagram.com/581066165581870/?locale=es_ES [Fecha de consulta: 04 de diciembre de 2023].

activos en la UE tendrán obligaciones más estrictas, porque un gran tamaño conlleva una gran responsabilidad.»⁴⁴⁶

Por su parte Margrethe Vestager, vicepresidenta ejecutiva responsable de “Una Europa Adaptada a la Era Digital”⁴⁴⁷, indicó que:

«Con la Ley de Servicios Digitales, disponemos ahora de una legislación clara. Las plataformas en línea constituyen el núcleo de algunos de los aspectos clave de nuestra vida cotidiana, nuestras democracias y nuestras economías. Es lógico garantizar que estén a la altura de sus responsabilidades a la hora de reducir la cantidad de contenidos ilícitos en línea y limitar otros perjuicios en línea, así como de proteger los Derechos fundamentales y la seguridad de los usuarios.»⁴⁴⁸

De acuerdo con lo que se contempla en la Ley de Servicios Digitales (DSA), una vez que la ley sea de completa aplicación, las empresas se enfrentan, en caso de incumplimiento de la misma, a sanciones de hasta un 6 % de su facturación global anual. En el caso de que las infracciones sean reiteradas, las empresas infractoras incurren en riesgo de que se les prohíba su estancia en la Unión Europea, y así como operar dentro de la misma.⁴⁴⁹

Todas las medidas de carácter institucional que ha implementado la Unión Europea y que están orientadas a frenar y/o restringir el contenido delictivo y terrorista en Internet, poseen un denominador común: el fomento a la cooperación entre Estados, instituciones, agencias de la UE, policías nacionales, investigadores, socios de la UE⁴⁵⁰ y empresas de tecnología.

En los últimos cinco años ha existido un notable incremento del interés de estas últimas en trabajar de forma estrecha y colaborativa con las instituciones y agencias de la Unión. Sí bien la Ley de Servicios Digitales (DSA) ha impuesto un rigor legal a la relación que se establecía hasta el momento entre el sector público y privado, en las empresas prevalece un espíritu cooperativo orientado al fomento de la seguridad en Internet. Un ejemplo ilustrativo de ello es el desarrollo del Centro de Ingeniería de Seguridad de Google (GSEC)⁴⁵¹ que la empresa ha establecido en Málaga. El Centro de Ingeniería de Seguridad de Google (GSEC) de Málaga es el tercero de este tipo en el continente europeo. Existe un GSEC en Múnich (creado en 2019) y un GSEC en Zúrich (creado en 2021). El GSEC de Málaga no obstante sería el primer GSEC especializado en ciberseguridad de Europa. Una de las características que posee este GSEC será que además de desarrollar su trabajo como centro para combatir el cibercrimen, fomentará una

⁴⁴⁶ «La Unión Europea impondrá controles más estrictos a las grandes plataformas digitales», *Euronews*, edición online de 25 de abril de 2023. Disponible en: <https://es.euronews.com/my-europe/2023/04/25/la-ue-impondra-controles-mas-estrictos-a-las-grandes-plataformas-digitales> [Fecha de consulta: 03 de diciembre de 2023].

⁴⁴⁷ «Una Europa Adaptada a la Era Digital. Capacitar a las personas con la ayuda de una nueva generación de tecnologías», *Comisión Europea*. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es [Fecha de consulta: 04 de diciembre de 2023].

⁴⁴⁸ COMISIÓN EUROPEA (2022): *Comunicado de Prensa. Ley de Servicios Digitales: entran en vigor las normas determinantes de la UE para las plataformas en línea*, 16 de noviembre de 2022, Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_6906 [Fecha de consulta: 04 de diciembre de 2023]. Véase Índice: ANEXOS. Anexo N.º 04: *Comunicado de prensa: Ley de Servicios Digitales: entran en vigor las normas determinantes de la UE para las plataformas en línea*.

⁴⁴⁹ «La UE aprueba una nueva ley para frenar el contenido ilegal de plataformas como Facebook, Google o Amazon», *La Voz de Galicia*, edición online de 23 de abril de 2022. Disponible en: <https://www.lavozdeg Galicia.es/noticia/sociedad/2022/04/23/ue-aprueba-nueva-ley-frenar-contenido-ilegal-plataformas-facebook-google-amazon/00031650700928811380708.htm> [Fecha de consulta: 04 de diciembre de 2023].

⁴⁵⁰ Ref.: Terceros Estados.

⁴⁵¹ GSEC por sus siglas en inglés (*Google Safety Engineering Center*, - Centro de Ingeniería de Seguridad de Google-).

alianza con la comunidad local a través de diversos *stakeholders*⁴⁵² como la universidad local⁴⁵³, las incubadoras de empresas⁴⁵⁴, las empresas locales, etc., con el objeto de trabajar en objetivos comunes en torno a la seguridad en Internet y la seguridad global.⁴⁵⁵

Este trabajo colaborativo fomenta la relación de cooperación entre lo público y lo privado al desarrollar alianzas con instituciones nacionales y europeas, y con socios de terceros países. Ken Walker, presidente de Asuntos Globales de Google, ha explicado que el GSEC de Málaga será un “espacio de colaboración entre expertos, académicos, empresas y gobiernos europeos en el que discutir sobre buenas prácticas, compartir investigaciones y conocimientos y, en definitiva, conseguir avances en seguridad, que sean beneficiosos para todos.”⁴⁵⁶

Si bien el GSEC de Málaga es un centro especializado en ciberseguridad, y por tanto atenderá a todo tipo de demandas relacionadas con los ciberdelitos, su actuación no se circunscribe a los delitos informáticos de los particulares, sino que proveerá seguridad contra el ciberterrorismo. Por ello, existe por parte del GSEC una colaboración institucional con la UE orientada a frenar las amenazas a la seguridad global.

En la jornada de inauguración del GSEC, que tuvo lugar en Málaga el 28 de septiembre de 2023, se puso de manifiesto esta voluntad de la UE a través de las palabras de Dita Charanzová, vicepresidenta del Parlamento Europeo:

«El peligro es real y más grave de lo que el ciudadano medio puede sospechar. [...] Hay millones de amenazas detectadas cada día [...] contra empresas, instituciones y gobiernos. Y sus repercusiones no son solo financieras; minan la confianza de los ciudadanos e interfieren en la seguridad de las elecciones, y en nuestras democracias.»⁴⁵⁷

En consonancia con lo expresado por Charanzová⁴⁵⁸, el vicepresidente de la Comisión Europea, Margaritis Schinas, repasó las iniciativas en marcha que posee la UE para “consolidar el arsenal europeo para hacer frente a las ciberamenazas”, pero advirtió que no bastan las leyes, normas y

⁴⁵² Término anglosajón utilizado para definir a los públicos o grupos de interés respecto a una empresa, proyecto o iniciativa. Son todas aquellas personas o segmentos poblacionales (partes) con los que nos interese establecer un dialogo y/o comunicación fluida. Según Canelo Sanmartín, “*de las relaciones que pueden establecer los stakeholders o los públicos con las organizaciones, lo más importante en la comunicación institucional es la cognitiva, la cual está basada en la interacción y el conocimiento mutuo.*” Véase: CANELO SANMARTÍN, Mercedes (2017): *La comunicación en las fuerzas de seguridad*. Barcelona: UOC; p. 71.

⁴⁵³ Universidad de Málaga (UMA).

⁴⁵⁴ ECCRI CIC por sus siglas en inglés (*The European Cyber Conflict Research Incubator CIC*, -Incubadora Europea de Investigación sobre Ciberconflictos CIC-). ECCRI CIC es una organización de Reino Unido que funge como una incubadora de empresas. Posee alianza con GSEC, y se centra en el “*estudio interdisciplinario del impacto de las tecnologías digitales y emergentes en los asuntos globales, en Europa y más allá*”. Véase: The European Cyber Conflict Research Incubator. Disponible en: <https://europeancyber.org> [Fecha de consulta: 04 de diciembre de 2023].

⁴⁵⁵ «Google presenta en Málaga su tercer centro de ciberseguridad de Europa», *Escudo Digital*, edición online de 30 de noviembre de 2023. Disponible en: https://www.escudodigital.com/ciberseguridad/google-presenta-en-malaga-su-tercer-centro-ciberseguridad-europa_57346_102.html [Fecha de consulta: 04 de diciembre de 2023].

⁴⁵⁶ «Google abre en Málaga su primer centro especializado en ciberseguridad de Europa», *El País*, edición online de 29 de noviembre de 2023. Disponible en: <https://elpais.com/tecnologia/2023-11-29/google-abre-en-malaga-su-primer-centro-especializado-en-ciberseguridad-de-europa.html> [Fecha de consulta: 04 de diciembre de 2023].

⁴⁵⁷ En esta cita textual, Charanzová se refiere expresamente al hecho de que las amenazas digitales no se encuentran solamente en los delitos informáticos que deriven en pérdidas económicas para particulares y/o empresas, sino que las amenazas en Internet hacen auténtico daño a la seguridad global. Charanzová se refiere a las *fake news* al mencionar las interferencias a la seguridad de las elecciones y a la pérdida de confianza ciudadana, y se refiere al terrorismo y al extremismo político al expresar que hay peligros reales y más graves que atentan contra nuestras democracias.

⁴⁵⁸ «El bastión de defensa de Google en Andalucía», *Diario de Sevilla*, edición online de 4 de diciembre de 2023. Disponible en: https://www.diariodesevilla.es/tecnologia/bastion-defensa-Google-Andalucia-centro-seguridad-malaga-video_0_1853815506.html [Fecha de consulta: 04 de diciembre de 2023].

directivas. Indicó, por tanto, que en la erradicación de las amenazas en Internet “resulta clave el trabajo coordinado y conjunto. El éxito reside en el compromiso del sector privado, para entrenar a profesionales, y por eso estamos contentos de integrar a Google en este compromiso”.⁴⁵⁹

El GSEC de Málaga aspira a ser un pilar para crear un Internet y una Europa más segura, protegiendo estos espacios de las amenazas que se ciernen sobre la seguridad global. En este sentido, el trabajo desarrollado por Google junto a la UE materializa parte de las iniciativas público-privadas que vienen teniendo lugar en los últimos años dentro de la lucha contra el uso de Internet con fines terroristas y contra el ciberterrorismo.

Todo parece indicar que el desarrollo institucional, normativo y preventivo de la UE en esta materia tenderá a la cooperación ya no solo con otras instituciones europeas o EEMM, sino primordialmente con el sector privado.

En la actualidad, la Política Criminal de la UE integra, en su lucha contra el terrorismo, a actores no institucionales y no europeos, como son las empresas o los socios de terceros Estados, atendiendo de esta manera a la propia naturaleza global de Internet. El monitoreo de Internet, que implique el análisis de material yihadista y el análisis de las ciberamenazas del terrorismo, cuenta con una variedad de actores que exceden las fronteras de la Unión. Serán todas las partes interesadas, las que mediante el trabajo conjunto permitan adoptar medidas operativas que tiendan a la restricción y a la erradicación de estos contenidos.

⁴⁵⁹ *Ibidem*.

CAPÍTULO 7: MEDIDAS PREVENTIVAS EUROPEAS DESTINADAS A EVITAR EL RECLUTAMIENTO YIHADISTA ONLINE Y LOS EXTREMISMOS EN INTERNET

LA PREVENCIÓN DEL TERRORISMO MEDIANTE EL DISEÑO DE POLÍTICAS PÚBLICAS

La Política Criminal de la Unión Europea ha adoptado, además de las medidas normativas y operativas previamente descritas, una serie de medidas de carácter preventivo que han ido orientadas a brindar información y a concienciar a la población europea sobre los riesgos que supone la existencia de extremismos violentos, debido al hecho de que estos habitualmente representan la antesala a diversas comisiones delictivas y/o acciones terroristas.

Las medidas de carácter preventivo que ha implementado la Unión Europea en toda la región se han focalizado principalmente en la creación y difusión de campañas de comunicación preventiva basadas en el contradiscurso terrorista, así también como en intervenir de forma favorable para modificar las situaciones o condiciones que representan un riesgo o vulnerabilidad para un grupo, y que, debido a ello, lo predisponen al terrorismo.

Teniendo en cuenta estas premisas, la Unión Europea ha diseñado políticas públicas que sustentan un modelo preventivo orientado a reducir el terrorismo en Europa, y a minimizar el impacto sobre la población europea del radicalismo yihadista online. Para Inmaculada Marrero Rocha, la gran capacidad de la Unión Europea como organización internacional ha fomentado una “europeización de la prevención de la radicalización”, y ha permitido que la prevención “haya adquirido un gran dinamismo y esté teniendo resultados en la generación de conocimiento, teórico y práctico, y en la identificación de las mejores prácticas para diseñar estándares de prevención que puedan ser útiles para todos”.⁴⁶⁰

Antes de continuar avanzando en esta exposición cabe introducir una explicación conceptual acerca de los modelos preventivos del delito.

Tradicionalmente, las medidas de prevención han sido percibidas dentro de la Política Criminal de un Estado como medidas de poca efectividad y de muy alta inversión económica. Debido a ello, habitualmente la mayor parte de los países han desarrollado frente al delito medidas de punición normativa o medidas que tienden a la consolidación del aparato represivo institucional. El primer tipo de medidas, las que son llevadas a cabo por medio de la vía normativa, representan en términos generales la opción más barata para un Estado, por lo que suele ser la opción más utilizada, y debido a ello, dicho Estado debe de cuidar en extremo de no realizar una excesiva utilización de su Derecho penal, a fin de no caer en una expansión del mismo. Esto último implicaría que el Estado busque resolver por la vía normativa problemas que pueden (y en ocasiones deben) ser abordados por otro medio.

El segundo tipo de medidas requiere de un mayor presupuesto estatal, que se suele justificar en el hecho de poder otorgar efectividad a las medidas de carácter normativo previamente mencionadas. El razonamiento para esta mayor erogación presupuestaria que realiza el Estado se basa en el entendimiento de que una norma sin la fuerza coercitiva que proporciona el aparato

⁴⁶⁰ MARRERO ROCHA, Inmaculada (2022): «La prevención de la radicalización violenta de corte yihadista en la Unión Europea», en: *Revista de Derecho Comunitario Europeo*, 73, (793-828), p. 820.

institucional carece de absoluta significancia porque no se garantiza su cumplimiento. El segundo tipo de medidas promueve entonces un amplio espectro institucional, nutrido a través de diversas agencias, centros, fuerzas de seguridad, policías, unidades especiales de inteligencia, etc., que, de forma mecanicista y legalmente facultado, persigue, reprime y reduce el delito.

En este binomio de ley-intuiciones parece resumirse gran parte de las medidas adoptadas dentro de la Política Criminal de muchos de los Estados frente al delito.

Las medidas normativas e institucionales señaladas comparten la característica sobre la necesidad de que el delito ya haya tenido lugar, es decir que ya se hubiera producido, para que se consideren medidas aplicables. Por el contrario, las medidas de carácter preventivo tienden a anticiparse al hecho, y su cometido radica en intervenir antes de que se produzca el delito con el objeto de eliminar o reducir al máximo los factores que facilitan o incitan a su comisión.

Desde esta perspectiva de Peter Lejins⁴⁶¹ explica que tanto las medidas normativas como las medidas institucionales son en sí mismo también medidas preventivas. Para Peter Lejins, la prevención del delito dentro de un Estado se aborda de tres maneras: por medio de la denominada prevención punitiva⁴⁶², que implica el entramado de acciones legítimas que derivan sobre el individuo de la interacción entre el Derecho penal de un Estado, sus fuerzas de seguridad, su sistema penitenciario y su sistema judicial. También por medio de la denominada prevención mecánica⁴⁶³, como un tipo de prevención que está caracterizada por la cibervigilancia, la vigilancia ciudadana, la prevención del delito mediante el diseño ambiental⁴⁶⁴, los sistemas de control aleatorio, la bases de datos, el desarrollo de software, redes tecnológicas de seguridad, automatizaciones, control de accesos, uso de inteligencia artificial, etc. Y finalmente, por medio de la denominada prevención correctiva⁴⁶⁵, que se orienta al fomento del empleo, la inclusión social, el arraigo o contención, la orientación y asesoría a grupos vulnerables, las campañas informativas, la educación, y a todas aquellas medidas que permitan anticiparse a la comisión delictiva.

Hacia este modelo preventivo, que Peter Lejins ha denominado correctivo, se orientó buena parte de la Política Criminal de la Unión Europea, y se buscó con ello orientar a los Estados Miembros para que pudieran erradicar, dentro de sus territorios nacionales, los factores primigenios que determinan la existencia del terrorismo.

Es decir, los tres tipos de medidas se orientan a prevenir el delito: las medidas normativas tienden a desanimar la acción delictiva por medio de la punición, y las medidas institucionales estableciendo trabas o dificultando la comisión (por ejemplo, en Internet). Pero son únicamente las medidas preventivas aquellas que pueden impedir de forma concreta que el hecho delictivo tenga lugar, dado que las otras medidas son expresamente respuestas a las acciones terroristas.

En el marco del desarrollo de las medidas consideradas exclusivamente preventivas, por su carácter anticipatorio, la Unión Europea se ha centrado en adoptar acciones dentro de lo que se

⁴⁶¹ LEJINS, Peter (1967): «The field of prevention», en: AMOS, William E./WELLFORD, Charles F. (Eds.), *Delinquency prevention: Theory and practice*, Englewood Cliffs: Prentice-Hall.

⁴⁶² Peter Lejins denomina prevención punitiva a la utilización del Derecho penal o a cualquier tipo de medida normativa. Véase: VIRGINIA DEPARTMENT OF CRIMINAL JUSTICE SERVICES (2018): *Crime Prevention History and Theory*, Course, Day 1 Session 2, DCJS, (1-69), pp. 28-31. Disponible en: <https://www.dcjs.virginia.gov/sites/dcjs.virginia.gov/files/training-events/5318/2020-2crimepreventionhistory-theory-dcjs.pdf> [Fecha de consulta: 24 de noviembre de 2023].

⁴⁶³ Lejins se refiere aquí a las medidas operativas de carácter institucional que hemos analizado previamente. Véase: *Ibidem*.

⁴⁶⁴ *Crime Prevention Through Environmental Design (CPTED)*.

⁴⁶⁵ Medidas preventivas propiamente dichas, en cuanto se sitúan temporalmente antes de la comisión delictiva.

conoce como P/CEV (Prevención o combate al extremismo violento).⁴⁶⁶ Dentro del modelo preventivo de P/CEV se engloban las acciones de PEV (Prevenir el extremismo violento) y de CEV (Combatir el extremismo violento). Las acciones de PEV tienen objeto de prevenir los extremismos y la radicalización, mientras que las acciones de CEV se orientan al combate de los dichos extremismos. En el primer caso, mediante las actividades de PEV, estamos ante un contexto de intervención preventiva a fin de evitar que un sujeto vulnerable⁴⁶⁷ sea radicalizado. En el segundo caso nos encontramos en un contexto de intervención rehabilitadora, conforme el sujeto ya se encuentra inmerso en un proceso de extremismo y/o de radicalización. Sin embargo, cabe señalar que el hecho de que un sujeto se encuentre transitando un proceso de radicalización no implica necesariamente que haya cometido un acto terrorista. De hecho, las acciones de CEV trabajan precisamente en una línea preventiva ulterior en donde se trata de evitar por todos los medios de intervención posibles que un sujeto ya radicalizado cometa un atentado. Fatima Lahnaït comenta al respecto,

«A lo largo de las últimas dos décadas, la lucha contra el extremismo violento a nivel mundial ha consistido, sobre todo, en medidas antiterroristas basadas en la seguridad, adoptadas con el fin de reducir/disuadir/combater la amenaza que plantean los grupos extremistas violentos. Es desde hace tan solo unos pocos años que se aplican métodos más amplios e integrales para analizar los factores y causas por las que hay individuos que ingresan en grupos extremistas violentos. Los programas CEV, por ejemplo, combaten procesos de radicalización que conducen al extremismo violento, no al terrorismo. Su propósito es el de movilizar y capacitar a ciertos agentes que, tradicionalmente, no tenían relación con la seguridad nacional, tales como administraciones locales, educadores, trabajadores sociales y sociedad civil. El objetivo es tanto concienciar como dotar de resiliencia a aquellas personas consideradas potencialmente vulnerables, o «en riesgo», con el propósito de prevenir la radicalización y el extremismo violento (PEV), así como de apoyar a quienes se han radicalizado, pero han decidido abandonar el extremismo (lo que se ha denominado «desradicalización»). Estas medidas comprenden campañas para la opinión pública, capacitación de comunidades, programas de prevención específicos –orientados en particular a colegios y centros de enseñanza, universidades, asociaciones o clubes juveniles y deportivos, centros religiosos, centros penitenciarios (considerados «viveros» de la radicalización), centros de refugiados– e Internet).»⁴⁶⁸

Para comprender la orientación de estas prácticas, podemos remitirnos a la clasificación habitual utilizada en las actividades de P/CEV que se realiza teniendo en cuenta el modelo de salud pública de Caplan⁴⁶⁹ en el cual aplica la psiquiatría clínica. Dicho modelo, en el cual se trata la

⁴⁶⁶ Dicha práctica preventiva engloba a su vez las actividades específicas de PEV (Prevenir el extremismo violento), por medio de las cuales se actúa antes de que una persona se radicalice, y de CEV (Combatir el extremismo violento), cuyas actividades están orientadas a la intervención para lograr la desradicalización, y rehabilitación o reinserción, de una persona que ya ha sido radicalizada.

⁴⁶⁷ La vulnerabilidad de un sujeto no representa ninguna connotación positiva o atenuante de su conducta desviada. La connotación de ‘vulnerable’ viene dada por el hecho de que el sujeto se encuentre expuesto a factores que puedan actuar como desencadenante de la comisión delictiva. Ejemplo de ello es la falta de arraigo social -comunidad, país de residencia, centros deportivos, culturales, etc.-, la falta de arraigo familiar, la falta de educación o empleo, etc., instituciones todas ellas que actúan como preventivas del delito.

⁴⁶⁸ LAHNAÏT, Fatima (2021): «Prevenir el extremismo violento para combatir el yihadismo autóctono: aprender de la experiencia», *Revista de Ciencias Sociales Iconos* 71, vol. XXV, N.º 71, septiembre-diciembre 20, FLACSO, Ecuador, (43-57), pp. 45-46.

⁴⁶⁹ El modelo de salud pública de Gerald Caplan fue expuesto en 1964 en “su legendario libro *Principios de Psiquiatría Preventiva*, que se convirtió en un texto de referencia en el desarrollo de las reformas comunitarias en salud mental, tanto para los planificadores como para los clínicos. Resulta curioso cómo la mayor parte de sus planteamientos, aunque siguen vigentes, se han desatendido en la deriva que han tomado los servicios de salud mental hacia una atención individualizada, medicalizada y desconectada de la comunidad de la que forman parte. Caplan considera que la psiquiatría preventiva es parte de un esfuerzo comunitario más amplio que la propia disciplina, en el cual los psiquiatras aportan sus contribuciones especializadas a una totalidad mayor.” [...] “Caplan plantea que la prevención primaria es un concepto comunitario: no trata de evitar que se enferme un individuo en especial, sino de reducir el riesgo de toda una población. Contrasta, pues, con la salud mental orientada hacia el paciente individual. El modelo conceptual se basa en

conducta desviada de un individuo, se mantiene en vigencia en gran parte de los programas preventivos del delito. Según dicho modelo, “la prevención primaria pretende evitar que se produzca una conducta desviada en un sistema ‘no infectado’, e incluye actividades orientadas, por ejemplo, a la sensibilización general, la resiliencia u otras formas de cohesión de la comunidad.”⁴⁷⁰

El tratamiento preventivo del terrorismo yihadista desde esta perspectiva clínica permite el abordaje temprano en tres fases. En términos generales, la prevención del delito basada en P/CEV se estratifica en una prevención primaria, secundaria y terciaria. Dentro de estos estratos se ordenan diferentes acciones específicas. Según Koehler,

«La prevención primaria se centra en las personas –y los problemas sociales– antes de que entren en contacto con individuos y grupos extremistas y se articulen riesgos específicos. La prevención secundaria, por su parte, pretende evitar la cristalización de los factores de riesgo o el proceso de radicalización en estadios precoces. Y la prevención terciaria pone el foco en prevenir la recaída en el extremismo violento u otras conductas de riesgo, lo que implica que se ha conseguido previamente un desistimiento inicial o desvinculación.»⁴⁷¹

Dentro de estas tres categorías, el trabajo se aborda con metodologías específicas y adecuadas según el estadio en el que se encuentre el sujeto. Influye para esto también el rango etario, dado que, por ejemplo, no reciben el mismo tratamiento metodológico de desradicalización los adultos que los niños.

Sin embargo, en donde no se establece una diferenciación tan notoria es entre los propios programas de PEV y CEV. Al respecto, Koehler enuncia que, “en la práctica, no existen diferencias claras entre las metodologías y los programas orientados a la prevención y aquellos orientados a la intervención, es decir, entre PEV y CEV, ya que los procesos de radicalización no son lineales”, y según el autor, al contrario de lo que sucede en el discurso académico, en la práctica profesional resulta difícil o incluso “imposible decidir si una persona todavía no es lo ‘suficientemente radical’ como para una intervención” del tipo CEV.⁴⁷² Todo ello hace que las intervenciones preventivas posean una gran abanico de posibilidades según el sujeto sobre el cual tiene incidencia. Podría decirse que si bien hay orientaciones generales de cuando deben tener lugar las actividades PEV y cuándo deben tener lugar las intervenciones CEV, las mismas

*la hipótesis de que para no sufrir un problema mental la persona necesita continuos aportes adecuados a las diversas etapas de crecimiento y desarrollo: aportes físicos, que incluyen alimentación, vivienda, estimulación sensorial, oportunidad de ejercicio, etc.; y aportes psicosociales, que incluyen la estimulación del desarrollo intelectual y afectivo de una persona por medio de la interacción personal con los miembros significativos de la familia y con los iguales y superiores de las instituciones sociales.” [...] “En este punto, la acción social es la tarea que modifica los sistemas operativos sociales y políticos, y la actividad legislativa reguladora relativa a la salud, la educación y el bienestar, con el fin de mejorar a escala comunitaria la provisión de aportes físicos, psicosociales y psicoculturales básicos, y la organización de servicios para ayudar a los individuos a enfrentar sus crisis. El profesional de salud mental tendría que ofrecer consejo a legisladores y administradores, y colaborar con otros ciudadanos para influir en instituciones gubernamentales y cambiar las normas y reglamentos. La acción social incluye los esfuerzos para modificar las actitudes generales y la conducta de los miembros de la comunidad a través de los medios de comunicación, el sistema educativo, etc. y mediante la interacción entre los sectores profesional y lego. Su labor también es asesorar a los líderes comunitarios, ampliando su visión en los aspectos concernientes a la salud mental de los asuntos que tratan, y colaborar con grupos de presión de ciudadanos que realizan campañas políticas para reclamar mejoras desde un posicionamiento activista.” Véase: ORTIZ LOBO, Alberto (2019): «Contra la prevención sanitaria individual del sufrimiento mental», *Revista de la Asociación Española de Neuropsiquiatría*, vol.39 no.135, ene./jun. 2019, (177-191), pp. 186-187.*

⁴⁷⁰ KOEHLER, Daniel (2021): «La desradicalización en Alemania: prevenir y combatir el extremismo violento», *Revista CIDOB d’Afers Internacionals*, N.º 128, (59-79), p. 62.

⁴⁷¹ *Ibidem*.

⁴⁷² *Ibidem*, p. 63.

poseen toda clase de adecuaciones conforme a la fase de radicalización que se encuentre atravesando el sujeto, la edad que posea, la comunidad a la que pertenezca, etc. En cualquier caso, los profesionales que están en contacto con el individuo son los que deben decidir qué tipo de método es necesario utilizar conforme a los requerimientos individuales de la situación que atraviesa el sujeto.

«Normalmente, se combinan las herramientas orientadas a la prevención [PEV] con aquellas orientadas a la intervención [CEV] para conseguir efectos en todos los niveles: a) prevenir una mayor radicalización, b) reducir el compromiso psicológico y físico hacia el ambiente radical y/o influir en el patrón de pensamiento o ideología, c) evitar recaer en la violencia y el extremismo, d) aumentar la resiliencia hacia los grupos y las ideologías extremistas, y e) ayudar a forjar una identidad y una vida nueva y autosuficiente.»⁴⁷³

En el marco de la lucha antiterrorista que se lleva a cabo actualmente en la Unión Europea, este tipo de medidas que le son propias al modelo P/CEV, se desarrollan activamente por medio de la implementación de diversas políticas públicas a fin de prevenir el reclutamiento, combatir el terrorismo violento y promover la desradicalización.

Como ya se ha mencionado, las medidas CEV (Combatir el extremismo violento) se dirigen particularmente a los terroristas y a los individuos extremistas radicalizados, es decir, hacia aquellos que se encuentran inmersos en el yihadismo. Por el contrario, las medidas PEV (Prevenir el extremismo violento) se orientan a evitar la captación de sujetos que por sus condiciones de vulnerabilidad podrían ser un potencial objeto de reclutamiento por parte del yihadismo. Existe, por tanto, en las medidas PEV, cierto grado de predictibilidad. Los cuerpos profesionales que deben aplicar estas medidas se encargan de considerar ciertas variables predictivas (arraigo familiar, salud, educación, integración, bienestar social, desarrollo psicosocial y psicocultural), que, de acuerdo con el grado de desarrollo o deterioro de tales variables en un individuo, permite detectar y anticiparse a un potencial riesgo de reclutamiento de dicha persona. Es fundamental para desarrollar este trabajo preventivo la multidisciplinariedad del cuerpo profesional. Debido a ello, el mismo suele estar compuesto por trabajadores sociales, docentes de todos los niveles educativos, profesionales de psicología y psiquiatría, profesionales de la salud, coordinadores de prevención, miembros de cuerpos policiales, funcionarios de centros penitenciarios y criminólogos. A su vez, estos profesionales trabajan de forma colaborativa con los referentes comunitarios, la familia del sujeto en riesgo, grupos de iguales del sujeto, y los líderes de opinión locales, así también como miembros o líderes religiosos que promuevan una visión del islam no violento. Estos grupos que son parte del ambiente socioafectivo del sujeto a su vez permiten la actuación de una prevención comunitaria.⁴⁷⁴

Las medidas P/CEV difieren en el público al cual se orienta. Las medidas de CEV se orientan a individuos condenados por terrorismo o manifiestamente terroristas, y las medidas de PEV a individuos vulnerables a un reclutamiento terrorista. No obstante, aun cuando posean una metodología diferente en cada caso, se utilizan los mismos instrumentos. Entre todos ellos el

⁴⁷³ *Ibidem*.

⁴⁷⁴ MEDINA ARIZA, Juanjo (2010): «Políticas de seguridad ciudadana en el contexto urbano y prevención comunitaria. La experiencia anglosajona», en: *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 12-02 (1-36), p. 14-18.

más utilizado es el contradiscurso o contranarrativa. “Las contranarrativas son relatos que pretenden erosionar la legitimidad de narrativas extremistas de carácter violento (NEV).”⁴⁷⁵ Según Miravittlas Pous, existen tres tipos de contranarrativas, estas son, la comunicación estratégica gubernamental⁴⁷⁶, las narrativas alternativas y las narrativas de choque. La comunicación estratégica gubernamental es promovida por el gobierno y se orienta a informar a la población acerca de cuáles son las acciones que se están llevando a cabo para contrarrestar el extremismo violento. Las narrativas alternativas son discursos o historias que se presentan como opción válida a las NEV.⁴⁷⁷ Y finalmente las narrativas de choque, son aquellas que buscan deslegitimar las NEV y sus portavoces mediante el cuestionamiento del sistema de creencias, el descrédito, la deconstrucción del relato, etc.⁴⁷⁸

Las contranarrativas surgieron como una herramienta dentro de la metodología P/CEV con la intención de afectar la capacidad de reclutamiento del yihadismo, y de alterar la legitimidad y el apoyo hacia las NEV. Suponen, dentro del ámbito preventivo, una formulación estratégica diferente conforme se trabaja en el ámbito de las ideas y el sistema de creencias del individuo. Las contranarrativas utilizan Internet, de igual modo que lo hacen los terroristas para propagar su mensaje, por lo tanto, estos mensajes orientados a la deslegitimación del discurso yihadista cuentan con las mismas ventajas de inmediatez y multiplicación del mensaje.

Desde su aparición, las contranarrativas han gozado de gran aceptación porque han supuesto no solo un modelo preventivo de abordar el fenómeno del terrorismo, sino también la idea de hacerlo en el mismo plano en el que opera el yihadismo, el ideológico. Desde la contranarrativa se busca no solo llevar adelante una acción preventiva, sino principalmente desarrollar una ofensiva ideológica que busca erosionar y reducir el mensaje del terrorismo en Internet.

Tal magnitud posee este enfoque que países como Estados Unidos de América y Reino Unido, pioneros en la materia, han desarrollado unidades específicas de contranarrativa terrorista dentro de su aparato estatal. En el año 2007 Reino Unido creó la *Research, Information and Communications Unit* (RICU)⁴⁷⁹ y en el año 2011 Estados Unidos de América creó el *Center*

⁴⁷⁵ MIRAVITLLAS POUS, Enric (2015): «Hacia una tipología de contranarrativas frente al extremismo violento», en: *Actas de XII Congreso de la Asociación Española de Ciencia Política y de la Administración*, organizado por AECPA, celebrado en Euskal Herriko Unibertsitatea, Universidad del País Vasco, San Sebastián, 13 a 15 de julio de 2015, (1-21), p. 1.

⁴⁷⁶ Cabe señalar que la comunicación estratégica gubernamental, se lleva a cabo siempre que un gobierno desee comunicarse con su público (ciudadanía, un sector específico de la población, usuarios de determinados servicios públicos, un grupo etario poblacional, etc.) por cualquier motivo que sea de interés para las partes. La comunicación estratégica gubernamental no se limita únicamente a desarrollar medidas o contranarrativas antiterroristas, sino que se utiliza para comunicar una gran variedad de temas de interés público. Por ejemplo, la comunicación estratégica fue ampliamente utilizada por muchos gobiernos del mundo para hacer frente a la crisis sanitaria del Covid-19. En términos generales, la comunicación estratégica (gubernamental, empresarial, o institucional) es un herramienta comunicativa que cualquier ente interesado en su *target* puede gestionar con el objeto de transmitir información y de lograr el entendimiento con su público objetivo.

⁴⁷⁷ “La función de una narrativa alternativa es cambiar la dirección de una conversación particular e introducir algo novedoso donde hasta ahora pueden haber dominado narrativas obsoletas, ofensivas o incluso aparentemente irrelevantes. [...] Desde sus inicios, el lado práctico del desarrollo de una narrativa alternativa se ha vuelto más refinado, ayudado en parte por el desarrollo del modelo GAMMMA+. El modelo GAMMMA+ ofrece directrices prácticas para desarrollar campañas alternativas y contranarrativas eficaces. El modelo ha sido promovido por el Grupo de Trabajo de Narrativas y Comunicación de RAN (RAN C&N) desde diciembre de 2017 y, en su versión más reciente (noviembre de 2019), se compone de siete elementos clave: Objetivo, Audiencia, Mensaje, Mensajero, Medios, Acción, más Monitoreo y Evaluación.” Véase: CARTHY, Sara (2021): *Lessons Learned from Alternative Narrative Campaigns*, RAN External Expert, European Commission, (1-20), pp. 4-6.

⁴⁷⁸ *Ibidem*.

⁴⁷⁹ La Unidad de Investigación, Información y Comunicaciones (*Research, Information and Communications Unit*, RICU) tiene como objetivo principal comprender y contrarrestar las ideologías terroristas y extremistas para reducir el riesgo para Reino Unido, sus ciudadanos y sus intereses en el extranjero. Véase: HAYES, Ben/ QURESHI, Asim (2016): *We Are Completely Independent. The Home Office, Breakthrough Media and the Prevent Counter Narrative Industry*, Report, London: CAGE.

for Strategic Counterterrorism Communications (CSCC) que ha sido reemplazado en el año 2016 por el *Global Engagement Center* (GEC).⁴⁸⁰ Ambas unidades, RICU y GEC (ex CSCC), diseñadas por su respectivos gobiernos, poseen una gran dotación de profesionales de diversas disciplinas científicas, y comparten el objetivo de trabajar contra las acciones del terrorismo en Internet mediante una comunicación estratégica eficaz, que se apoya instrumentalmente en el monitoreo de la red, en las contranarrativas, en un posicionamiento ideológico definido, y en la información veraz.

Reino Unido y Estados Unidos de América actuaron como países pioneros en el desarrollo de la contranarrativa gubernamental. En la actualidad, la contranarrativa es utilizada por gran parte de los Estados que sostienen una lucha abierta contra el terrorismo yihadista internacional. Si bien la herramienta es la misma, se plantean en los usos de la contranarrativa particularidades discursivas que son inherentes al Estado o ente supranacional que la desarrolle.

La Unión Europea también ha incorporado el contradiscurso dentro de sus medidas preventivas. El contradiscurso europeo posee una orientación que concentra sus esfuerzos en erosionar el marco ideológico de la narrativa extremista, a la par que desarrolla una comunicación estratégica focalizada en el fortalecimiento de sus Estados Miembros, por medio de su apoyo institucional y su soporte financiero destinado a la prevención de los radicalismos en cada Estado parte.

En el marco de las políticas públicas preventivas hacia el terrorismo, la Unión Europea mantiene una profusa comunicación interna con sus EEMM a fin de guiar a estos en sus esfuerzos contra el terrorismo y su vez impulsar la armonización regional de la lucha antiterrorista en este ámbito. Para llevar a cabo esta empresa, la Unión Europea actúa hacia cada uno de sus Estados Miembros como un promotor de las campañas preventivas nacionales, como una fuente de financiación, y como una fuente de referencia y conocimiento en cuanto al funcionamiento de los radicalismos y extremismos en Europa, así como la prevención a adoptar frente a estos.

Desde hace más de una década, Europa se ha centrado en la investigación del funcionamiento del extremismo y el radicalismo en la región, en el afán de poder desarrollar políticas preventivas que se adecuen a las amenazas en Internet. Para la Unión Europea,

«Es imposible desarrollar una respuesta certera a las amenazas emergentes del extremismo violento sin comprender las fuerzas que mueven ese proceso. La investigación llevada a cabo al nivel de la UE puede suponer un valor añadido cuando su objetivo es ubicar y analizar las grandes tendencias de radicalización. [Por ello,] es preciso seguir investigando para comprender cómo y por qué se radicalizan o desradicalizan los individuos. Esta investigación debe abordar los papeles que desempeñan la ideología, las nuevas técnicas de captación a través de Internet y los ‘modelos de rol’.»⁴⁸¹

⁴⁸⁰ El Centro de Comunicaciones Estratégicas Antiterroristas (*Center for Strategic Counterterrorism Communications*, CSCC) se creó en el año 2011 como una empresa pública para coordinar, orientar e informar sobre las actividades de comunicación externa que realizaba el gobierno estadounidense para combatir el terrorismo y el extremismo violento. En el año 2016, fue reemplazado por el Centro de Participación Global (*Global Engagement Center*, GEC) e incorporado a la Oficina de Asuntos Públicos Globales del Departamento de Estado. La actual misión de GEC se centra en liderar los esfuerzos del gobierno de los EE. UU. para "reconocer, comprender, exponer y contrarrestar los esfuerzos de propaganda y desinformación estatales y no estatales extranjeros destinados a socavar o influir en las políticas, la seguridad o la estabilidad de los Estados Unidos, sus aliados y naciones asociadas" en todo el mundo. Véase: «About Us – Global Engagement Center», *US Department of State*. Disponible en: <https://www.state.gov/about-us-global-engagement-center-2/> [Fecha de consulta: 29 de noviembre de 2023].

⁴⁸¹ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Prevenir la radicalización hacia el terrorismo y el extremismo violento: una respuesta más firme de la UE, (COM/2013/941 final), p. 11.

Este interés en la investigación de los radicalismos y los extremismos en Internet ha llevado a la Unión Europea a crear, en el marco de su Política Criminal preventiva, diversas estructuras y/o redes, orientadas a comprender, sintetizar y a guiar a los Estados Miembros para que desarrollen acciones acordes al modelo preventivo que propone la Unión. De todas las iniciativas que han surgido como productos de esta temprana investigación, existen dos de particular interés e impacto preventivo que son la *Radicalization Awareness Network* (RAN)⁴⁸² y la *European Strategic Communications Network* (ESCN)⁴⁸³.

La Red de Sensibilización sobre la Radicalización (*Radicalization Awareness Network*, RAN) fue creada en el año 2011, a iniciativa de la Comisión Europea. La RAN se encarga de conectar entre sí a “profesionales de toda Europa, como psicólogos, docentes, trabajadores sociales, agentes de policía, funcionarios de prisiones, funcionarios de ministerios, y agentes de libertad vigilada, que trabajan directamente con personas vulnerables a la radicalización y con personas que ya se han radicalizado.”⁴⁸⁴ El proyecto RAN es una ‘red paraguas’, o red de redes, y proporciona una plataforma para que los profesionales reúnan y compartan mejores prácticas en la lucha contra la radicalización que conduce al extremismo violento.

La RAN tiene como finalidad ayudar y capacitar a aquellos profesionales que se encuentran en la primera línea del trabajo preventivo, con el objeto de que estos sean capaces de luchar contra la radicalización. Además, la RAN se encarga de asesorar a políticos y académicos de los Estados europeos, a fin de que estos sean portavoces de las acciones y labores que se llevan a cabo por medio de esta red. El objetivo último de RAN es reintegrar a los extremistas violentos y para ello recurre al “fomento del intercambio de experiencias, por ejemplo, en reuniones y conferencias, el uso de herramientas prácticas pertinentes, y la difusión de información y especialización.”⁴⁸⁵ La RAN también produce una serie de publicaciones, que se comparten con su red de profesionales de primera línea, que destacan las lecciones aprendidas, las ideas y las recomendaciones de las reuniones del Grupo de Trabajo y consolidan el conocimiento y la experiencia de la RAN. Desde su fundación en 2011, la RAN ha atraído a más de 6.000 profesionales, que representan colectivamente a todos los Estados Miembros de la UE.⁴⁸⁶

La Red Europea de Comunicaciones Estratégicas (*European Strategic Communications Network*, ESCN) es una red, fundada por la Comisión Europea en el año 2016, donde los expertos de los Estados Miembros de la Unión Europea comparten buenas prácticas y análisis sobre comunicación estratégica para prevenir y contrarrestar las acciones del extremismo violento. La red posee un equipo consultivo permanente que asesora a los gobiernos sobre cómo crear una estrategia de comunicación que posicione al Estado contra el terrorismo y

⁴⁸² «RAN Policy Support», *European Commission*. Disponible en: https://home-affairs.ec.europa.eu/networks/ran-policy-support_en [Fecha de consulta: 30 de noviembre de 2023].

⁴⁸³ «La Red Europea de Comunicaciones Estratégicas (ESCN), un proyecto liderado por Bélgica inició operaciones en octubre de 2016. Se basa en el trabajo anterior del Syria Strategic Communication Advisory team (Equipo Asesor de Comunicación Estratégica de Siria, SSCAT). La ESCN está formada por representantes de instituciones estatales de al menos 19 Estados Miembros de la UE. Está cofinanciado por la subvención de acción del Fondo de Seguridad Interior-Policía (ISF-Policía).» Véase: EUCPN (2019): *European Crime Prevention Monitor 2019/1: Radicalisation and violent extremism*. Brussels: European Crime Prevention Network.

⁴⁸⁴ TRIBUNAL DE CUENTAS EUROPEO (2018): «Hacer frente a la radicalización que conduce al terrorismo: la Comisión respondió a las necesidades de los Estados Miembros, pero con algunas deficiencias en la coordinación y la evaluación», Informe Especial N.º 13, (1-37), p. 12

⁴⁸⁵ *Ibidem*.

⁴⁸⁶ «Radicalisation Awareness Network», *Real Instituto Elcano*. Disponible en: <https://www.realinstitutoelcano.org/en/projects/radicalisation-awareness-network/> [Fecha de consulta: 30 de noviembre de 2023].

sobre la producción de campañas de contranarrativa. ESCN es a la vez una red y una plataforma de comunicaciones para expertos en P/CEV que trabajan en instituciones estatales de toda la Unión Europea para el intercambio de conocimientos y experiencias prácticas con diversos sectores, incluido el mundo académico.

La ESCN también se encarga de identificar socios creíbles para las intervenciones públicas y se ha dedicado a explorar el papel de los medios de comunicación tradicionales en la lucha contra las narrativas extremistas violentas. Ambas situaciones se deben al hecho de que la Política Criminal de la Unión Europea, dentro de sus acciones preventivas, ha considerado también el enfoque mediático en el abordaje de sus políticas públicas orientadas a combatir el yihadismo. El papel que cumplen los medios de comunicación europeos en la prevención del terrorismo yihadista ha sido señalado reiteradamente por la Red Europea de Comunicaciones Estratégicas (ESCN) como limitado. Si bien la ESCN y el proyecto RAN trabajan en la difusión de contranarrativas en Internet, los Estados Miembros vinculados a ambas redes valoran positivamente la incorporación de los medios de comunicación tradicionales dentro de las políticas públicas de prevención, para ayudar en dicha difusión. Los medios de comunicación son considerados por la población europea como socios creíbles, y pueden, por lo tanto, fortalecer la comunicación estratégica antiterrorista. Tal es dicho interés, que, en el año 2016,

«Las autoridades belgas informaron al Tribunal de que en el marco estratégico no se abordaba de manera suficiente la cuestión de los medios convencionales (televisión, radio y prensa). Consideraban importante incluir esta cuestión para facilitar la reflexión sobre el papel de los medios, no solo en la incitación a las personas a abandonar Europa para luchar en Siria, sino también en la contribución a la polarización en la sociedad, lo que podría crear tensiones que conducen a la radicalización.»⁴⁸⁷

Mario Toboso Buezo considera imprescindible incorporar a los medios de comunicación dentro de las políticas públicas preventivas, pero considera que antes debe existir lo que denomina ‘pedagogía de los medios’. Es decir, los medios deben de estar sujetos a una línea comunicativa estratégica a fin de que logren la finalidad preventiva y sean capaces de transmitir la contranarrativa de forma fiel a los intereses de la Unión Europea. Para Toboso Buezo, la pedagogía de los medios involucra que los mismos tengan en cuenta los siguientes lineamientos:

- «1. La cobertura desmesurada genera conclusiones precipitadas, información no contrastada y largas tertulias ricas en superlativos que, a menudo, provocan efectos perversos. La demanda de información y el afán por aportar datos – no siempre contrastados– en tiempo real pueden favorecer el clima de vulnerabilidad, alarmismo, caos y ansiedad perseguido por los terroristas.
2. Fomentar el lenguaje preciso de los términos evitando el exceso de eco mediático y la saturación de determinados fenómenos (kamikazes, infraestructuras críticas, guerra, lobo solitario, inmoliación, cerebro...).
3. Evitar proyectar una imagen de supremacía de DAESH o Al Qaeda informando de sus derrotas, desertiones o de la mortalidad de sus líderes operativos e ideológicos. La erosión de DAESH evita la proyección de poderío y de éxito que seduce a miles de jóvenes musulmanes vulnerables.
4. [Evitar] Ponderar la difusión de los videos propagandísticos yihadistas para evitar la amplificación del mensaje terroristas, la humillación de las víctimas y la percepción de que cada ejecución o el asesinato de personas es banal. Filmar la ejecución de una persona indefensa es un acto de vileza y cobardía ajeno a cualquier halo de creatividad que algunos enfoques parecen sugerir.

⁴⁸⁷ TRIBUNAL DE CUENTAS EUROPEO (2018), opus cit., p. 18.

5. Potenciar el papel de la víctima y su relato vital frente a la exaltación del verdugo.
6. La difusión reiterada de fotografías de terroristas así como la divulgación pormenorizada de su relato vital puede tener un efecto contraproducente ya que podrían ser ejemplarizados por individuos que experimenten un proceso de extremismo violento o de aceptación de la narrativa yihadista.
7. Insistir en el hecho objetivo de que la mayoría de las víctimas del terrorismo yihadista son musulmanes.
8. [Evitar] Ponderar el ‘tertulianismo’ y promover la difusión de un mensaje ajeno a estereotipos o generalidades que pueden contaminar la esencia de la amenaza. La colaboración con expertos del mundo académico que trabajan en proyectos de investigación de disciplinas vinculadas, directa o indirectamente, con el fenómeno del terrorismo permiten la difusión de un mensaje objetivo, ponderado y riguroso.
9. La insistencia del argumento de la sinrazón terrorista puede ser percibida como un signo de vulnerabilidad.»⁴⁸⁸

Para Toboso Buezo, los medios de comunicación tienen un papel fundamental en la comprensión de la amenaza. “Si la información es rigurosa no se sobredimensiona la amenaza, y si el lenguaje es preciso no se fomenta la incertidumbre y el miedo tiene muchas más dificultades para propagarse.”⁴⁸⁹

En la actualidad, el mundo académico, el sector político y profesionales expertos en P/CEV parecen coincidir en la necesidad de incorporar a los medios de comunicación dentro de las políticas públicas preventivas que coordina la Unión Europea. Como máximo referente de la comunicación gubernamental, dentro del propio Club de Venecia se mencionó la necesidad de establecer relaciones con los medios de comunicación y de promover “el establecimiento de un clima de confianza mutua y transparencia como condición previa para evitar percepciones e interpretaciones erróneas de las actividades de comunicación de las autoridades públicas.”⁴⁹⁰

En el marco de los diálogos del Club de Venecia, a tenor de esta alianza gobiernos-medios de comunicación, cuya finalidad sea la difusión de la contranarrativa europea, se expusieron reflexiones que han quedado recogidas en la publicación *Convergences N.º 10*. En dichas conclusiones se sintetizan en los siguientes puntos:

- «Los continuos riesgos de polarización de la sociedad, el aumento del extremismo, los sofisticados medios de propaganda terrorista, la interdependencia entre diferentes grupos terroristas y el riesgo de explotación de la crisis migratoria y de refugiados con fines de reclutamiento siguen causando grandes preocupaciones de seguridad en la población. (véanse las tendencias del Eurobarómetro, que muestran el terrorismo como el tema que más preocupa a los ciudadanos).
- El desafío de las comunicaciones está cambiando rápidamente y esto requiere inversiones en capacidades de investigación dedicadas y capacidad para estudiar la naturaleza cambiante de las comunicaciones extremistas.
- Los gobiernos no pueden hacer esto solos, pero se necesitan nuevas asociaciones entre los gobiernos, la sociedad civil, las industrias y las empresas de Internet y medios de comunicación. La confianza es crucial. Un “programa de empoderamiento de la sociedad civil” propugnado por la Comisión Europea podría ayudar a cumplir este propósito.
- Siguiendo el enfoque de organizaciones como SSCAT (que está cambiando su denominación a la más inclusiva “Red Europea StratComms” - ESCN), se alienta encarecidamente a los Estados Miembros a fomentar las relaciones entre expertos en comunicación para intercambiar cada vez más experiencias y desarrollar la capacidad de analizar, investigar y desarrollar contranarrativas.

⁴⁸⁸ TOBOSO BUEZO, Mario (2016): «Una aproximación a la contranarrativa yihadista», *Grupo de Estudios de Seguridad Internacional, GESI*, Universidad de Granada, p. 6.

⁴⁸⁹ *Ibidem*.

⁴⁹⁰ CLUB OF VENICE (2017): *Convergences N.º 10: Public Communication in Europe*, (1-136), p. 21

- Las contranarrativas, sin embargo, sólo hacen una parte del trabajo. De hecho, se requiere todo un conjunto de respuestas para desafiar la narrativa de los extremistas y restaurar la confianza entre audiencias clave.
- La respuesta debe coincidir con el ritmo y la escala del desafío. Esto sólo puede suceder mediante la construcción de una arquitectura formal interna para impulsar una entrega diaria, consistente y coherente de comunicaciones, incluidas las campañas.
- Existe una gran necesidad de una evaluación continua del impacto, con el fin de ajustar y optimizar las campañas de información y comunicación en curso y mantener un enfoque proactivo continuo.»⁴⁹¹

Las relaciones con los medios de comunicación por parte de las instituciones europeas y de los Estados Miembros, desde este prisma estratégico que permita el desarrollo de contranarrativas desde un punto de vista preventivo, representa un desafío futuro. Sí bien la perspectiva está puesta en solventar todas las dificultades que pueden derivarse de esta asociación gubernamental-profesional, el principal desafío parece radicar en el propio paradigma actual de los medios de comunicación que se debaten entre la inmediatez de los hechos noticiosos del terrorismo yihadista, y la rigurosidad informativa a la que aspira la Unión Europea como una arista más de sus políticas preventivas.

LAS MEDIDAS DE INTERVENCIÓN, LAS CAMPAÑAS DE INFORMACIÓN Y LAS ACCIONES DE CONTRANARRATIVA YIHADISTA EN INTERNET ADOPTADAS DENTRO DE LA UNIÓN EUROPEA.

La Unión Europea desarrolla una gran cantidad de medidas de intervención y campañas de carácter preventivo orientadas a la información y a la contranarrativa. Las campañas se desarrollan por medio de organizaciones o redes que pertenecen a la esfera pública (como, por ejemplo, RAN), o por medio de entes privados tales como *think tanks*, organizaciones no gubernamentales, asociaciones comunitarias, etc. En términos generales, las organizaciones que se ocupan de la radicalización violenta no son ‘nuevas’ ni se crearon *ad hoc* para abordar este fenómeno. Según *Youth Partnership*⁴⁹²,

«Sus enfoques a menudo difieren, pero tienen algo en común: su respuesta a la radicalización que conduce a la violencia no es la de ‘extinguir incendios’ (una respuesta rápida a un problema puntual), sino más bien holística y arraigada en una comprensión amplia de la situación, rol, valores y prácticas del trabajo juvenil, teniendo una perspectiva de largo plazo del aprendizaje y desarrollo de los jóvenes.»⁴⁹³

El modelo de prevención que suelen llevar adelante todas las organizaciones que trabajan en este campo, suelen centrar sus prácticas en los primeros pasos de la radicalización potencial que conduce a un posterior proceso de violencia. Para ello, se suele recurrir al modelo Moghaddam.⁴⁹⁴

⁴⁹¹ *Ibidem*.

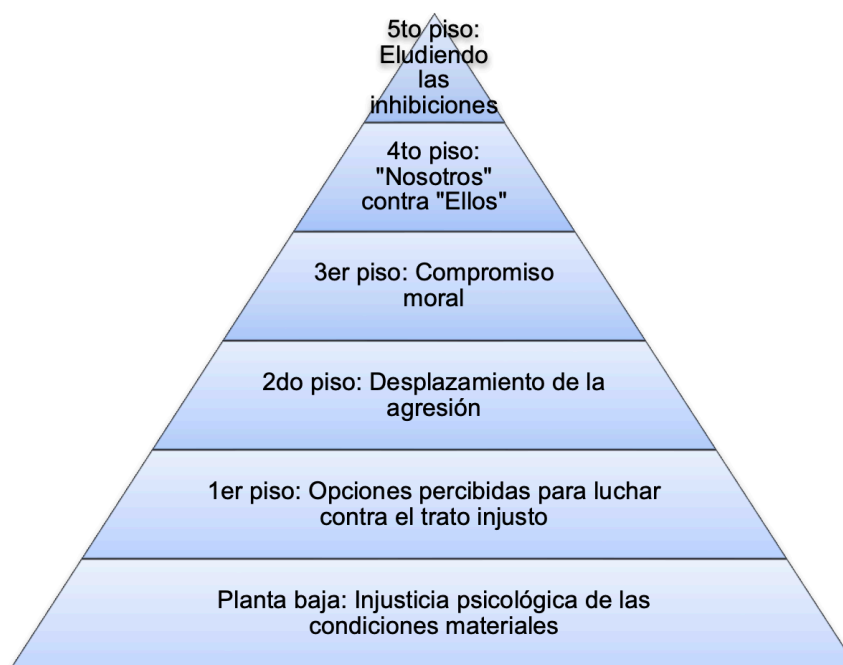
⁴⁹² *Youth Partnership* es una asociación entre la Comisión Europea y el Consejo de Europa dedicada al ámbito de la juventud. Véase: «*Youth Partnership*», *Council of Europe and European Union*. Disponible en: <https://pjp-eu.coe.int/en/web/youth-partnership> [Fecha de consulta: 30 de noviembre de 2023].

⁴⁹³ GARCÍA LÓPEZ, Miguel Angel/ PAŠIĆ, Lana (2018): *Youth work against violent radicalisation. Theory, concepts and primary prevention in practice*, Council of Europe and European Commission, April 2018, (1-82), p. 27.

⁴⁹⁴ MOGHADDAM, Fathali M. (2009): «De-Radicalization and the Staircase from Terrorism», en CANTER, David (Ed.), *The Faces of Terrorism: Multidisciplinary Perspectives*, New Jersey: Wiley, pp. 277-292.

El modelo Moghaddam pretende mostrar que la radicalización que conduce a la violencia es el resultado de procesos que inician en la sociedad, y que representan para el individuo una escalera que se estrecha, reduciendo sus opciones. No considera todas las formas posibles de violencia, solo considera los segmentos determinantes de los procesos de radicalización que conducen hacia la violencia. Dichos segmentos, según Moghaddam, se observarían de forma gráfica de la siguiente manera:

Gráfico 7: El “modelo escalera” del terrorismo



Fuente: Fathali M. Moghaddam.

Aunque existen diferentes trayectorias y caminos individuales hacia la radicalización que conduce a la violencia, para Fathali Moghaddam es posible identificar seis pasos por los que los jóvenes pueden pasar mientras atraviesan el proceso de radicalización violenta.

Los caminos de cada persona pueden ser bastante diferentes, y las transiciones de uno a otro pueden no ser tan claras, pero estos seis pasos ayudan a comprender algunos de los caminos personales hacia la formación de creencias radicales y hacia actos violentos, así como como por qué los individuos pueden involucrarse o no en el proceso de radicalización. Es importante destacar que no todos los individuos que atraviesan las primeras etapas alcanzan el nivel de radicalización violenta. Si bien estos segmentos representan una escalera, es posible la movilidad, y avanzar o retroceder dentro de este modelo.

Básicamente el modelo de Moghaddam consta de seis segmentos o pisos. Estos son: Planta baja (La planta baja se encuentra integrada por todos los miembros de la sociedad. Dentro de esta planta baja que representa a la sociedad los individuos autoevalúan sus condiciones de vida. Influyen negativamente en esta autoevaluación la percepción subjetiva de privaciones, injusticia, inmovilidad social, las amenazas a la identidad, y la influencia de los medios de comunicación difundiendo el sentimiento de injusticia), Primer piso (En el primer piso, los sujetos consideran su situación personal y opciones para mejorar su situación. Ello involucra

dos aspectos, en primer lugar, la percepción limitada de posibilidades de movilidad social, y en segundo lugar las formas alternativas de mejorar la situación. Se tiene en este estadio la percepción de que los procedimientos judiciales son injustos y tendenciosos. Esta percepción genera una idea de injusticia e ilegitimidad hacia el sistema normativo vigente. La agresión sentida se proyecta así hacia el ‘otro’, considerado como responsable de los problemas), Segundo piso (El segundo piso implica el surgimiento en el individuo de sentimientos de ira y frustración por no poder mejorar su situación. Surge un objetivo al que culpar y se produce el desplazamiento de la agresión, que en esta etapa es verbal y física. Esto se refleja en el apoyo directo o indirecto de grupos u organizaciones que defienden y promueven una visión de ‘nosotros contra ellos’), Tercer piso (En el tercer piso, los sentimientos de ira y frustración pueden ser capitalizados por una organización de extremismo violento ofreciendo un compromiso con el individuo, que se ve inmerso en un proceso de nueva identidad mediante la persuasión y la justificación de los medios para lograr la sociedad ideal. Se emplean tácticas de aislamiento, afiliación, confidencialidad y miedo. Las organizaciones que capitalizan estos sentimientos de ira o frustración poseen dos niveles: el nivel macro, como única opción para cambiar el mundo o reformar la sociedad, y el nivel micro, como un refugio para los indignados, los descontentos, los marginados y otras personas que se encuentran en situaciones similares), Cuarto piso (En el cuarto piso el grupo promueve el pensamiento dicotómico ‘nosotros contra ellos’ y aumenta el aislamiento del sujeto respecto de sus familiares y/o amigos. Se enfatiza la legitimidad de la organización y tiene inicio un proceso de intrasocialización secreta), Quinto piso (En el quinto piso tiene lugar la fase operativa en donde se llevan a cabo los actos violentos. La organización utiliza los recursos necesarios para inhibir los mecanismos que impiden al sujeto realizar acciones violentas. Se determina una categorización social para el ‘otro’, que se utiliza para identificarlo como el objetivo y el enemigo. Despersonalización de las otras personas, y exageración de diferencias entre el grupo intra -organización- y extra -sociedad percibida como enemiga-).⁴⁹⁵

Teniendo en cuenta el análisis de los factores que influyen en la radicalización que conduce a la violencia, la gran mayoría de las campañas informativas y de los programas de rehabilitación y desradicalización europeos actuales abordan la prevención considerando los aspectos personales, laborales, educativos y sociales, que propone el modelo de escalera de Moghaddam. En el caso de los jóvenes, además de los factores mencionados, se tienen en cuenta también los sentimientos de exclusión, la falta de oportunidades percibidas, y otros aspectos personales como crisis de identidad, así también como la fuerte influencia de Internet en este grupo etario.

Muchas de las campañas de información o intervención preventiva son ilustrativas de este abordaje. Para que una campaña preventiva tenga éxito deben de tenerse en cuenta diversos factores que atañen al marco profesional del trabajo desarrollado por los expertos en P/CEV, dado que,

«todo proyecto, y en particular una medida para prevenir la radicalización sólo puede llevarse a cabo con éxito dentro de un marco determinado. Por lo tanto, es prioritario llegar a un acuerdo entre la dirección

⁴⁹⁵ *Ibidem.*

del proyecto y los participantes en el proyecto sobre las condiciones marco apropiadas y necesarias para alcanzar un objetivo común.»⁴⁹⁶

A continuación, de entre la gran variedad de programas preventivos existentes en los diferentes países de Europa que han sido financiados por la Unión Europea⁴⁹⁷ y que han registrado casos de desradicalización, citaremos algunos ejemplos a modo ilustrativo.

AKRAN (Alemania).⁴⁹⁸ El proyecto AKRAN está dirigido por *Kreuzberg Initiative against Antisemitism* (KIgA). El objetivo de AKRAN es la educación entre pares. AKRAN significa "par" en turco y en árabe. Jóvenes educadores entre pares de entre 18 y 28 años, de origen musulmán, cercanos al grupo destinatario de la organización y a sus experiencias de vida, participan en un proceso educativo con otros jóvenes. AKRAN utiliza un enfoque holístico para prevenir la discriminación y la radicalización que conducen a la violencia, incluida la prevención del yihadismo violento y la sensibilización de los jóvenes sobre la propaganda en Internet.

CoCoRa (Italia y Dinamarca).⁴⁹⁹ La Comunidad contra la radicalización (*Community Counteracting Radicalisation*, CoCoRa) es un proyecto europeo, cofinanciado por el programa Erasmus+ de la Comisión Europea. Su objetivo es desarrollar y probar una nueva estrategia de prevención basada en la comunidad que involucre a las comunidades locales y a los ciudadanos de origen musulmán directa y activamente en la prevención de la radicalización y el extremismo violento a través del proceso de empoderar a los jóvenes de estas comunidades para que sientan pertenencia y ciudadanía igualitaria. El proyecto CoCoRa promueve un enfoque adaptado al contexto local. Los socios del proyecto han implementado una variedad de enfoques comunitarios, que van desde la colaboración con una organización musulmana local, la colaboración transversal dentro de un área geográfica limitada, en asociaciones cívicas y ONG, en clubes juveniles e instituciones de integración, etc. Todos los enfoques comunitarios tienen en común el fuerte enfoque en el intercambio interreligioso e intercultural y en la capacitación en diálogo apreciativo, inclusión sociocultural y cuestiones de igualdad, ciudadanía autoincluida a través de la conciencia de derechos y deberes, empoderamiento y construcción de autoestima y desarrollo de valores positivos. comunidades con visiones propias. Actúa también como un foro para el aprendizaje cognitivo, así como para discusiones y reflexiones comunes sobre temas como la radicalización, las posiciones minoritarias, la ciudadanía democrática y la antidiscriminación.

MAKS VZW (Bélgica).⁵⁰⁰ La Acción Mediática de la Ciudad de Kuregem (*Media Actie Kuregem Stad*, MAKS VZW) utiliza herramientas digitales para contrarrestar la radicalización islámica y el discurso de odio, como la narración digital, la codificación u otras técnicas cinematográficas para aumentar la ciudadanía global, convirtiendo a los jóvenes en prosumidores en lugar de consumidores de dispositivos, utilizando la tecnología para permitir

⁴⁹⁶ RADICAL ONLINE EDUCATION (2017): *How to prevent radicalization*, Digital guide, Project Co-funded by the Erasmus+, Programme of the European Union, October 2017 to March 2019, Danish Youth Team (Denmark), Projuven (Spain), OEJAB (Austria), Alternativi International (Bulgaria), by Danish National Agency for Higher Education.

⁴⁹⁷ Véase Índice: ANEXOS. Anexo N.º 05: *Medidas contra la radicalización financiadas por la UE*.

⁴⁹⁸ AKRAN. Disponible en: <https://www.kiga-berlin.org> [Fecha de consulta: 30 de noviembre de 2023].

⁴⁹⁹ Community Counteracting Radicalisation (CoCoRa). Disponible en: www.mhtconsult.dk y www.cesie.org [Fecha de consulta: 30 de noviembre de 2023].

⁵⁰⁰ Media Actie Kuregem Stad (MAKS VZW). Disponible en: www.maksvzw.org [Fecha de consulta: 30 de noviembre de 2023].

su movilidad social y también abordando la propaganda. de los reclutadores de Dáesh que buscan jóvenes vulnerables. La narración digital es la práctica de utilizar herramientas informáticas para contar historias; es una narrativa personal en línea en formato digital. Al igual que con la narración tradicional, la mayoría de las historias digitales se centran en un tema específico y contienen un punto de vista particular, utilizando una combinación de imágenes, texto y audio grabados en computadora. Las historias pueden variar en duración, normalmente entre uno y cinco minutos, y las elabora y edita el narrador.

Vilvoorde (Bélgica).⁵⁰¹ Vilvoorde trabaja concretamente en P/CEV. Esta organización decidió que el punto de partida para esto fuera un triángulo de prevención, utilizado en criminología y educación, con diferentes niveles, incluida la sociedad, los servicios generales del gobierno local, la educación, la prevención del delito, el trabajo juvenil, las medidas de prevención específicas, la intervención y la ley. El Servicio Municipal de Radicalización y Polarización de la Ciudad de Vilvoorde es un amortiguador entre los servicios sociales más amplios y la aplicación de la ley, y se ocupa de un tema específico. La idea es trabajar desde un enfoque no basado en conflictos, asumiendo que un asunto puede abordarse y solucionarse antes de que se convierta en un problema, y centrándose en resolver las frustraciones existentes, incrementando para ello la necesidad de generar confianza dentro de la comunidad e involucrar a la mayor cantidad posible de personas.

International Institute for Human Rights and Peace (Francia).⁵⁰² El Instituto Internacional para los Derechos Humanos y la Paz (*International Institute for Human Rights and Peace*) utiliza tres pilares: 1) Educación en derechos humanos a través de la educación no formal. La educación no formal es particularmente eficaz con los jóvenes que pueden haber sido atraídos hacia la violencia por grupos radicalizados, ya que les permite compartir sus experiencias, particularmente porque los jóvenes involucrados en la radicalización pueden no tener acceso a, o ser reticentes a la educación formal. 2) Usar modelos positivos al trabajar con jóvenes. Por ejemplo, en un proyecto con la administración de protección de menores, los menores bajo orden judicial se reúnen con profesionales para ayudarlos a descifrar los mecanismos utilizados por ciertos grupos radicales con la finalidad de captarlos. 3) Utilizar el arte para el proceso de aprendizaje. Los jóvenes pueden expresar sus sentimientos sobre el tema a través del arte. Por ejemplo, el Instituto trabajó con jóvenes rurales para abordar ciertos estereotipos (sobre inmigrantes o musulmanes) que pueden ser conducentes a una radicalización. Después de expresar por medio del arte los sentimientos que les provocaban dichos estereotipos, los jóvenes podían discutir de manera más racional los hechos, las realidades y sus experiencias.

Además de las iniciativas nacionales unilaterales, existen proyectos europeos en los que participa más de un Estado Miembro de la Unión Europea. Desde hace años en el Proyecto CoPPRa (*Community Policing Preventing Radicalisation*)⁵⁰³

⁵⁰¹ Stad Vilvoorde. Disponible en: www.vilvoorde.be [Fecha de consulta: 30 de noviembre de 2023].

⁵⁰² International Institute for Human Rights and Peace. Disponible en: www.2idhp.eu [Fecha de consulta: 30 de noviembre de 2023].

⁵⁰³ Community Policing Preventing Radicalisation (CoPPRa). Disponible en: https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/coppra_en [Fecha de consulta: 30 de noviembre de 2023].

«participan diversos países miembros de la Unión Europea con el objetivo de prevenir la radicalización ofreciendo a los agentes de proximidad formación para poder detectar procesos de radicalización. El contacto positivo entre la policía, los ciudadanos y las comunidades promueve la confianza con las instituciones. Una mayor confianza en la policía deriva en el hecho que la comunidad fomente la cooperación y la participación en programas de prevención. CoPPRa elabora manuales con directrices básicas sobre pautas de radicalización. El Modelo Aarhus⁵⁰⁴ es un proyecto institucional danés en el que participan diferentes actores: el Ayuntamiento de la localidad, la East Jutland Police, la Universidad de Aarhus o el PET⁵⁰⁵ entre otros. El objetivo principal del Modelo Aarhus es persuadir a los jóvenes que pretenden acudir a escenarios de conflicto y promover la reinserción de los que retornan siempre y cuando no hayan cometido delitos violentos. En el proyecto participa una red de profesionales de diferentes sectores como: trabajadores sociales, maestros, policías, voluntarios y familiares de los jóvenes radicalizados. La asesoría individual se complementa con mentores y talleres de concienciación. La aplicación del modelo, según los promotores, está teniendo cierta tasa de éxito, sobre todo en los estadios más tempranos del proceso de radicalización.»⁵⁰⁶

Otro ejemplo del trabajo preventivo que apoya financieramente la Unión Europea es aquel que se desarrolla ya no con el sujeto de interés, sino con la familia de este. En ocasiones, el individuo ha sido ya reclutado y no se encuentra, (ya sea porque se halla inmerso en un proceso de radicalización, privado de su libertad, fallecido, u otros factores que impiden la intervención P/CEV) en situación de ser rehabilitado. Frente a este hecho, la experiencia de reclutamiento y radicalización de estos sujetos puede ser transmitida por terceras personas, habitualmente su familia. Esta transmisión realizada por miembros cercanos de su familia puede actuar como un mecanismo inhibitorio para otros procesos de radicalización. Por ejemplo,

«La asociación *Moms for Life* formada por madres que han vivido los procesos de radicalización violenta de sus hijos relatan historias dotadas de una enorme carga sentimental y de credibilidad. Otro caso es el [...] grupo *Mothers Move!* [en donde la madre de Andrew Isa Ibrahim] participa a menudo en conferencias relatando el proceso de radicalización de su hijo.»⁵⁰⁷

En la actualidad existe además un importante factor de sensibilización vinculado al género. Cabe señalar que

«El número de mujeres radicalizadas durante los últimos años se ha incrementado de forma sustancial. En este sentido, el relato de una mujer que haya experimentado un proceso de radicalización o de una madre que haya protegido a sus hijos frente a la narrativa violenta son testimonios verosímiles y de una gran carga emocional.»⁵⁰⁸

En cualquiera de los casos en los que se apliquen, las medidas P/CEV actúan como un producto de intervención que se establece en todos los niveles, sensibilizando al sujeto con medidas de contranarrativa y por medio de su esfera microsocial, pero también creando una estructura que

⁵⁰⁴ «El Modelo de Aarhus es la estrategia para la prevención de la Radicalización y el Extremismo violento en la Ciudad de Aarhus, Dinamarca. El programa se centra en la prevención temprana de la radicalización y el extremismo. El trabajo llevado a cabo es una colaboración entre la Policía de Jutlandia Oriental y el municipio de Aarhus, y se lleva a cabo como complemento a las iniciativas de prevención del delito existentes. En la medida de lo posible, el trabajo utiliza iniciativas y procedimientos de prevención penal existentes, que se complementan con un grupo de trabajo interseccional e interdisciplinario con conocimientos específicos sobre radicalización. El Modelo Aarhus ofrece una variedad de intervenciones y esfuerzos hacia individuos, grupos, comunidades y el público en general, es decir, un programa de mentores, un programa de salida y actividades de creación de conciencia.» Véase: «The Aarhus Model», *Hedayah*. Disponible en: <https://hedayah.com/program/the-aarhus-model/> [Fecha de consulta: 30 de noviembre de 2023].

⁵⁰⁵ Servicio de seguridad e inteligencia danés.

⁵⁰⁶ TOBOSO BUEZO, Mario (2016), opus cit., pp. 5-6.

⁵⁰⁷ *Ibidem*, p. 12.

⁵⁰⁸ *Ibidem*.

produzca efectos antiterroristas específicos para el debilitamiento de los ambientes extremistas, como resulta ser Internet.

Desde hace años que, además de los modelos preventivos basados en contranarrativa, la prevención también se enfoca en medidas preventivas mecanicistas que de alguna forma interrumpen o debilitan el enlace del sujeto con las ideas extremistas y/o el radicalismo.

Por ejemplo, en el año 2016, durante la asistencia a unas Jornadas celebradas en Sevilla⁵⁰⁹, sobre el yihadismo actual y el uso de la inteligencia en HUMINT⁵¹⁰ y OSINT⁵¹¹ tuvo lugar una exposición en donde el ponente se refirió a *Risk-Track*,⁵¹² un software desarrollado por la Universidad Autónoma de Madrid que permite evaluar el riesgo de radicalización en redes sociales mediante la tecnología denominada AIDA (*Applied Intelligence and Data Analysis*).⁵¹³ Dicho software, fusionando conocimientos de lingüística, psicología, criminología y computación, pretende ser una herramienta semiautomática de análisis al servicio de distintos cuerpos de seguridad e inteligencia europeos, facilitando su labor de análisis, valoración de radicalización y toma de decisiones finales.

Otro ejemplo lo encontramos en el uso actual de la Inteligencia Artificial (IA) por parte de algunos de los proveedores de servicios de Internet, como YouTube, X (ex *Twitter*), etc., para bloquear contenido que los terroristas desean alojar en Internet. Como expone Manuel Torres Soriano, al presente:

“Los terroristas están sometidos a presión y a un entorno de hostigamiento digital por las medidas adoptadas por las plataformas que bloquean contenidos a través de herramientas como la inteligencia artificial que ayudan a mapear e identificar contenido yihadista en Internet.”⁵¹⁴

Sí bien la Inteligencia Artificial garantiza que ciertos contenidos yihadistas no puedan ser alojados en Internet, el uso de esta tecnología posee un sentido bidireccional. En la actualidad, la IA está siendo utilizada por el terrorismo en sustitución a los reclutadores tradicionales, lo que representa un problema sobre el control de Internet.

⁵⁰⁹ YIHADISMO ACTUAL: USO DE LA INTELIGENCIA EN HUMINT Y OSINT. (*Jornadas Exclusivas*). Organizado por GALEÓN-CISEG, 5 y 6 de octubre de 2016, Sevilla, España.

⁵¹⁰ HUMINT son las siglas de *Human Intelligence* (Inteligencia Humana) y es un término que se utiliza para describir la inteligencia o información clave recopilada de forma directa a partir de seres humanos. Implica un trabajo de inteligencia para obtener información de seres humanos concretos porque la respuesta solo es conocida por estos. Pude implicar técnicas de negociación, persuasión y/o manipulación.

⁵¹¹ OSINT es el acrónimo de *Open Source Intelligence* (Inteligencia de Fuentes Abiertas). Implica el trabajo de inteligencia mediante el uso de datos disponibles públicamente, que son recogidos por dispositivos electrónicos u otros medios. La OSINT suele proporcionar base informativa para desarrollar una buena HUMINT.

⁵¹² TORREGROSA, Javier (2016, 5 de octubre). «RISK-TRACK: Evaluando el riesgo de radicalización en redes sociales», en: *Jornadas Exclusivas sobre Yihadismo Actual: Uso de la inteligencia en HUMINT Y OSINT*. Organizado por GALEÓN-CISEG, 5 y 6 de octubre de 2016, Sevilla, España.

⁵¹³ “La experiencia de AIDA incluye: aprendizaje automático (agrupación, modelos ocultos de Markov, clasificación y aprendizaje profundo), inteligencia computacional (computación evolutiva, inteligencia de enjambre), modelado y minería de patrones y procesos, computación gráfica, análisis de redes sociales y comportamiento humano. modelado y minería. Actualmente, el grupo AIDA desarrolla actividades de investigación e innovación en áreas como Ciberseguridad y Ciberinteligencia, Detección de fake news y desinformación, Aeroespacial y tecnologías de Fusión de la Información.” Véase: *Applied Intelligence and Data Analysis (AIDA)*. Disponible en: <https://aida.etsisi.upm.es> [Fecha de consulta: 30 de noviembre de 2023].

⁵¹⁴ TORRES SORIANO, Manuel (2023, 16 de noviembre): «Panel 2: Tendencias de la amenaza en las sociedades occidentales», en: *X Foro Elcano Terrorismo Global “La nueva fase del terrorismo global: tendencias de la amenaza”*, Organizado por el Real Instituto Elcano, 16 de noviembre de 2023, Madrid, España.

Sin embargo, más allá de la utilización de la Inteligencia Artificial de la que hace uso el yihadismo, es representativo de éxito en materia de políticas públicas el aumenamiento de las medidas preventivas mecanicistas y de contranarrativa.

Esta naturaleza híbrida de las medidas de P/CEV, garantizan el desarrollo integral de una lucha contrterrorista eficaz, dado que las medidas de contranarrativa por sí solas no alcanzan a desarrollar todo el halo preventivo al que la Unión Europea aspira.

Además, resulta preciso señalar que las medidas de contranarrativa han despertado en algunos sectores cierto escepticismo acerca de su eficacia, e incluso también algunas críticas por parte de los propios expertos en P/CEV debido principalmente a su enfoque discursivo restrictivo. Algunas de estas críticas provinieron desde la propia Red de Sensibilización sobre la Radicalización (*Radicalization Awareness Network*, RAN), creada por la Comisión Europea en 2011, por lo que se entiende que son críticas fundamentadas en el quehacer diario y en el conocimiento que proviene de la experiencia profesional de aquellos expertos que se encuentran en la primera línea de trabajo preventivo contra el extremismo violento y la radicalización yihadista. Las críticas sostienen que:

«La contranarrativa, según algunos expertos de RAN, no debe fomentar la polarización argumental ni enfocarse en términos de ‘ellos’ y ‘nosotros’, ni de ‘vencer’ o ‘ganar’ el relato, sino que debe apelar a la manipulación de los argumentos y de las emociones por parte de la narrativa violenta. Otra crítica bien fundamentada es la complejidad metodológica en la medición del impacto de la contranarrativa. A pesar de ser un objeto de estudio actual requiere de herramientas empíricas que puedan calibrar cuantitativa y cualitativamente su impacto. En este sentido, más allá de las visualizaciones o *checkings* de algunos instrumentos en la red desde el empirismo académico se vislumbra la necesidad de evaluar científicamente su verdadero impacto. No obstante, la pedagogía de la amenaza del primer nivel de acción sí que reduce objetivamente la incertidumbre de la amenaza.»⁵¹⁵

Otra de las situaciones que se han prestado para el cuestionamiento de la eficacia del contradiscurso en materia preventiva se debe a casos documentados, en Reino Unido, Alemania y Austria, en donde sujetos que habían tenido procesos exitosos de rehabilitación y desradicalización por medio de técnicas de contranarrativas guiadas dentro de modelos preventivos P/CEV, han acabado con posterioridad cometiendo atentados terroristas. Koehler, en una detallada revisión de estos casos, nos permite conocer que:

«El 29 de noviembre de 2019, Usman Khan, de 28 años, asistió en Londres a una conferencia académica sobre rehabilitación de presos. Al cabo de unas horas, el joven decidió perpetrar un ataque terrorista cerca del London Bridge apuñalando a cinco personas, dos de las cuales morirían más tarde. Tras el ataque, Khan fue abatido por un agente de policía y se descubrió que portaba un cinturón de explosivos que resultó ser falso, además de un brazalete electrónico, ya que hacía poco que había sido puesto en libertad y disfrutaba de un permiso penitenciario. El joven había sido detenido en 2010 y en 2012, siendo condenado por delitos de terrorismo que incluían un atentado con bomba. Se supo que Khan había finalizado un programa de rehabilitación penitenciario denominado ‘Intervención para una identidad sana’ y participado en otra iniciativa diseñada para facilitar la desvinculación del terrorismo a largo plazo.

Al cabo de un año, otros dos ataques terroristas fueron cometidos por individuos que habían participado en los denominados programas de desradicalización o programas para prevenir y combatir el extremismo violento (P/CEV), diseñados para disminuir el riesgo de violencia.

El 4 de octubre de 2020, el refugiado sirio Abdullah Al H., de 20 años, mató a una persona por apuñalamiento en Dresde, Alemania. En septiembre de ese mismo año, el joven había sido puesto en

⁵¹⁵ TOBOSO BUEZO, Mario (2016), opus cit., pp. 12-13.

libertad tras ser condenado a prisión por delitos extremistas cometidos anteriormente y, durante su estancia en la cárcel, había empezado a participar en un programa no gubernamental de desradicalización. Tras su excarcelación, se había reunido con sus orientadores, antes y después de perpetrar el ataque, hasta que la investigación policial desembocó en su detención.

Un mes después, el 2 de noviembre de 2020, el joven Kujtim Fejzulai, de 20 años y nacido en Austria, mató a cuatro personas en un tiroteo en Viena, antes de ser abatido por la policía. El perpetrador había sido puesto en libertad en diciembre de 2019, y se le había ordenado seguir una terapia de desradicalización como parte de su libertad condicional.

Los tres sucesos fueron protagonizados por delincuentes terroristas que habían sido excarcelados y habían reincidido en sus acciones extremistas, a pesar de que habían recibido seguimiento por parte de las autoridades y orientación en programas de desradicalización. Por supuesto, estos casos (y muchos otros comparables) intensificaron el debate público sobre la efectividad, la calidad y la tasa de éxito de dichos programas de rehabilitación, desvinculación o desradicalización de terroristas.»⁵¹⁶

Estos sucesos cuestionan la eficacia de los programas de rehabilitación y radicalización, y plantean la pregunta sobre si los programas de desradicalización pueden ser evaluados conforme a sus resultados. A priori,

«La respuesta a la pregunta ‘¿Cómo se puede evaluar un programa de desradicalización?’ Es simple: un programa de desradicalización funciona si las personas que lo completan renuncian al radicalismo y no reinciden. Sin embargo, los especialistas en evaluación dan respuestas más matizadas con varios tipos diferentes de evaluación:

- La evaluación de impacto intenta determinar si una intervención tiene el resultado deseado. En medicina, por ejemplo, se podría evaluar si un medicamento específico puede curar a los pacientes. Para demostrar que el medicamento es la causa de la cura, también se administra un placebo a un grupo de control.
- La evaluación pragmática implica descubrir si el programa cumple con las expectativas de sus diversas partes interesadas.
- La evaluación basada en la teoría estructura la evaluación en torno a una teoría que puede describir cómo el programa logra los resultados deseados u observados y representa esta información en forma de modelo lógico, diagrama, o diagrama de flujo.
- La evaluación de procesos tiene como objetivo dar cuenta de la brecha entre la planificación y la ejecución de un programa.
- La evaluación realista tiene como objetivo utilizar la observación empírica para comprender una intervención, centrándose específicamente en los mecanismos subyacentes de la intervención y la influencia del contexto.»⁵¹⁷

Con independencia de los resultados evaluativos, es preciso considerar que valorar negativamente la eficacia de los modelos preventivos, sin brindar la posibilidad de establecer enmiendas o correcciones, suelen actuar como una justificación o acicate para endurecer el Derecho penal de un Estado que busca resolver el problema del terrorismo primordialmente por la vía punitiva, mediante la creación de nuevas tipificaciones o el incremento de penas.

Sí bien la Unión Europea no posee un Derecho penal propio que sea de aplicación común en todos los Estados de la Unión, las acciones derivadas de sus aciertos o desaciertos políticos, decisiones presupuestarias, orientaciones en materia de seguridad y defensa, y Política Criminal, poseen impacto en cada uno de los Estados Miembros al momento de posicionarse estos últimos contra el delito de terrorismo, y todo ello promueve que sigan con mayor o menor fidelidad las orientaciones europeas en este ámbito.

⁵¹⁶ KOEHLER, Daniel (2021), opus cit., p. 60.

⁵¹⁷ HECKER, Marc (2021): Once a Jihadist, Always a Jihadist? A Deradicalization Program Seen from the Inside, Focus stratégique, N° 102 bis, Ifri, February 2021, (1-78), Pag. 23

Si las medidas de carácter preventivo, principalmente aquellas que atañen a la contranarrativa, son cuestionadas por la opinión pública europea e incluso por los propios miembros de la Unión Europea, como en el caso de RAN, se crea un impacto negativo que puede deslegitimar dicho trabajo en cada uno de los Estados.

No debe olvidarse tampoco el hecho de que tradicionalmente dentro de la Política Criminal de un país, suele existir una tendencia hacia la punición debido a que la utilización del Derecho penal como medida para resolver el delito resulta menos costosa para las arcas del Estado que otras opciones. Además, la punición o el incremento de penas en ocasiones se utiliza, habitualmente en periodos electorales, como argumento político para acabar con el crimen en una sociedad.

La Política Criminal goza de poseer en su haber de medidas normativas, medidas institucionales, y medidas preventivas. El acierto está en corregir las deficiencias de cada tipo de medidas sin prescindir necesariamente de alguna de ellas. Tampoco es conveniente desvirtuar la naturaleza de cada una de estas medidas, por ejemplo, con el populismo punitivo, con el exacerbamiento del aparato estatal o instituciones altamente represivas, o con la victimización del delincuente. Se tratarían estas de deformaciones de cada tipo de medida, que amenazaría la necesaria permanencia y legitimidad de cada una.

Debido a ello, y en el afán de evitar dichos defectos, en la actualidad la Unión Europea se orienta al establecimiento de medidas coherentes y apegadas al Estado de Derecho dentro del ámbito normativo, institucional y preventivo de su Política Criminal actual. En virtud de ello, la Unión Europea,

«invita a los Estados Miembros a tener en cuenta las recomendaciones de políticas teniendo en cuenta las prácticas existentes en sus países que podrían desarrollarse aún más para hacer frente a las nuevas necesidades y desafíos [y a fomentar] la cooperación intersectorial entre el trabajo juvenil y los departamentos de seguridad y justicia, el trabajo social y el sistema de educación formal, entre otros, seguir desarrollándolos e incorporándolos [al trabajo preventivo]. Las recomendaciones preparadas y presentadas en este documento deben leerse y utilizarse de acuerdo con las realidades nacionales y locales que difieren en toda la Unión Europea.»⁵¹⁸

Esta visión de la Unión Europea da cuenta de que en lucha contra el terrorismo en la región actúa como un referente común para los países de la Unión, pero no niega las particularidades nacionales que podrían derivar en diferencias entre los Estados de la Unión a la hora de abordar el fenómeno del yihadismo.

⁵¹⁸ EUROPEAN COMMISSION (2017): *The contribution of youth work to preventing marginalisation and violent radicalisation. A practical toolbox for youth workers & Recommendations for policy makers*, Results of the expert group set up under the European Union Work Plan for Youth for 2016-2018, Luxembourg: Publications Office of the European Union, (1-50), p. 47.

PARTE III: REVISIÓN COMPARADA DE LA POLÍTICA CRIMINAL DE TRES ESTADOS EUROPEOS REFERENTE AL USO DE INTERNET CON FINES TERRORISTAS

CAPÍTULO 8: ALEMANIA

LA POLÍTICA CRIMINAL DE ALEMANIA EN MATERIA DE TERRORISMO

Es indiscutible el hecho de que Alemania posee un vasto desarrollo del Derecho penal, y que el mismo ha ejercido gran influencia en la doctrina de otros Estados, debido a que las conclusiones de la dogmática jurídica penal alemana siempre han sido un referente para todos los países que han seguido la tradición germana. Debido a ello, y teniendo en cuenta que el desarrollo del Derecho penal de Alemania desde su inicio hasta la fecha implica un enorme compendio de análisis, solo nos detendremos en hechos puntuales o hitos significativos para la doctrina y su relación con el terrorismo.

La Política Criminal antiterrorista de Alemania surge en la década de 1970 vinculada a las acciones de terrorismo de la *Rote Armee Fraktion*. Según María del Mar Carrasco Andrino, “el legislador alemán en un primer momento se decantó por no crear una legislación especial al margen del Código Penal, precisamente en ese afán de no configurar el terrorismo como algo cualitativamente distinto a la delincuencia tradicional.”⁵¹⁹ No obstante, con el paso del tiempo el Estado alemán ha ido paulatinamente incorporando disposiciones legales que fueron creando poco a poco un Derecho penal excepcional de aplicación exclusiva a los actos interpretados como terroristas.

Un hecho significativo de la Política Criminal alemana ha estado vinculado a un momento de profunda reflexión científica en una discusión teórica, relativa al Derecho penal excepcional, planteada por Winfried Hassemer, Björn Burkhardt, George Fletcher, Otfried Höffe, Claus Roxin y Albin Eser. Dichos académicos organizaron, en 1999, un ciclo de conferencias en materia de Derecho penal, bajo el título “*Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende, Rückbesinnung und Ausblick*”⁵²⁰. En dicho ciclo de conferencias que se llevó a cabo en la Academia de Ciencias de Berlín-Brandenburg del 3 al 6 de octubre del citado año, tuvo lugar la presentación de diversas ponencias científicas.

Una de dichas ponencias, la pronunciada por Winfried Hassemer,⁵²¹ se presentó de forma conjunta con los comentarios y las observaciones que Günter Jakobs le hacía a dicha ponencia. Los comentarios de Jakobs quedaron recogidos en una monografía titulada “La ciencia penal ante los retos del futuro.”⁵²² En la misma, el penalista alemán Günter Jakobs se refiere ampliamente al denominado ‘Derecho penal del enemigo’, y señala que este ‘Derecho penal del enemigo’, o Derecho de excepción, implica la idea de una ‘tolerancia cero’ hacia determinados tipos de delitos dentro de la sociedad, y que en razón de esto, este Derecho de excepción se

⁵¹⁹ CARRASCO ANDRINO, María del Mar (2019): «Derechos fundamentales y legislación antiterrorista: ¿Qué hemos perdido en el camino?», Estudios penales y criminológicos, vol. XXXIX, (59-105), pp. 67-68.

⁵²⁰ “La ciencia alemana del Derecho penal ante el cambio de milenio. Reflexión retrospectiva y perspectiva de futuro”.

⁵²¹ Cuya autoría es de Albin Eser, Winfried Hassemer y Björn Burkhardt

⁵²² Original en alemán. Su traducción dio lugar a varios errores, por ello también se encuentra en español incorrectamente bajo el nombre de: “La autocomprensión de la ciencia del Derecho penal ante los desafíos del presente.”

instrumentaría como una amenaza hacia los enemigos de dicha sociedad. Ello es, hacia aquellos que se alejan del Derecho vigente.

Por su naturaleza grave, el delito de terrorismo se encontraría dentro de una categoría en donde la aplicación del ‘Derecho penal del enemigo’ estaría debidamente justificada. En Alemania, el terrorismo y otras formas graves de delincuencia organizada, principalmente de carácter internacional y urgente, han propiciado que los principios básicos procesales del Derecho penal, (como son la proporcionalidad, presunción de inocencia, debido proceso, y otros), queden en suspenso, mediante la existencia de este Derecho penal excepcional.

Jakobs no niega la existencia del Derecho penal excepcional, pero manifiesta que esto implica “la imposibilidad de una juridicidad completa”⁵²³ sencillamente porque el Derecho penal excepcional o ‘Derecho penal del enemigo’ es contrario a los principios liberales de un Estado de Derecho y a todos los derechos fundamentales reconocidos en declaraciones universales de derechos humanos.

No obstante, este Derecho penal excepcional sería aplicable a todos aquellos calificados como enemigos de la sociedad, del Estado o del sistema. Dicha calificación no sería aleatoria, sino que para Jakobs, enemigo es todo aquel cuyo comportamiento delictivo no es ‘incidental’, sino aquel que de una forma presumiblemente duradera “ha abandonado el Derecho y, por tanto, no garantiza el mínimo cognitivo de seguridad del comportamiento personal y demuestra este déficit a través de su comportamiento.”⁵²⁴ En resumen, ello significa que son enemigos quienes “de una manera presuntamente duradera, [...] no ofrecen una mínima seguridad en su comportamiento”⁵²⁵ social.

En consecuencia, y debido a las reflexiones sobre las formas graves de delito internacional que se acentúan en el S. XXI, y con la llegada en el tercer milenio del terrorismo yihadista, para Jakobs impera la necesidad de que existan dos modelos de legislación penal dentro del Estado, en donde uno sea aplicable a los ciudadanos (Derecho penal del ciudadano), y el otro sea aplicable a aquellos calificados como enemigos (Derecho penal del enemigo).⁵²⁶ Estos dos modelos penales, opuestos entre sí, se distinguirían uno del otro por medio de lo que Günther Jakobs establece como características que son “típicas del Derecho penal del enemigo”. Estas características son:

- «Amplio adelantamiento de la punibilidad, es decir, cambio de la perspectiva del hecho producido por la del hecho que se va a producir, siendo aquí ejemplificadores los tipos de creación de organizaciones criminales o terroristas [...] o del cultivo de narcóticos por parte de bandas organizadas.
- Falta de una reducción de la pena en proporción a dicho adelantamiento.
- Paso de la legislación de Derecho penal a la legislación de la lucha para combatir la delincuencia.
- Supresión de las garantías procesales.»⁵²⁷

⁵²³ JAKOBS, Günther (2004): «La ciencia penal ante los retos del futuro», MANSO, Teresa (Trad.), en: ESER, Albin/HASSEMER, Winfried/BURKHARDT, Björn (Coords.) / MUÑOZ CONDE, Francisco (Coord. versión española), *La ciencia del Derecho penal ante el cambio de milenio*, Valencia: Tirant lo Blanch, (53-63), p. 53.

⁵²⁴ *Ibidem*, p. 59.

⁵²⁵ TORRES DEL MORAL, Antonio (2014): «Seguridad y Estado de Derecho», en CASTRO-RIAL GARRONE, Fanny (Coord.), *Contribución de la Guardia Civil a la seguridad*, (35-52), p. 47.

⁵²⁶ *Ibidem*

⁵²⁷ JAKOBS, Günther (2004), opus cit. pp. 53-55.

Estas cuatro singularidades son, para Jakobs, determinadamente descriptivas de este tipo de modelo penal, y le hacen reflexionar sobre el hecho de que el denominado ‘Derecho penal del enemigo’, según sus palabras, “no es propiamente Derecho, y [por consiguiente] convendría delimitar de modo preciso su naturaleza conceptual, tal vez a-jurídica.”⁵²⁸ Acorde con las características enunciadas, esta naturaleza a-jurídica se pone de manifiesto en la pérdida que sufre el Derecho penal de sus principios y garantías básicos.

Jakobs no adopta una postura crítica hacia el Derecho penal de excepción, sino que básicamente manifiesta la necesidad de no denominarlo ‘Derecho’ por no estar dotado de los principios y garantías que le son propios e irrevocables a todo Derecho penal. Es decir, Jakobs adhiere al postulado de que el Estado debe poseer un Derecho penal especial, ello es el Derecho penal de excepción o ‘Derecho penal del enemigo’, para que sea aplicable a todos los casos en los que la seguridad pública así lo exija, como los delitos de terrorismo u otros graves delitos internacionales, formas delictivas que adquirieron no solo en Alemania, sino en todos los Estados, especial protagonismo a partir del cambio de milenio.

La existencia y adopción de este Derecho de excepción naturalmente implica el suspenso de determinadas garantías fundamentales propias de un Estado de Derecho, “sobre todo las de carácter penal material (principios de legalidad, intervención mínima y culpabilidad) y procesal penal (derecho a la presunción de inocencia, a la tutela judicial, a no declarar contra sí mismo, etc.) [...]”⁵²⁹ Aun así, Jakobs considera que la Política Criminal alemana, con relación al delito de terrorismo, debe admitir la existencia de un modelo penal diferencial en aras de una utilidad y funcionalidad que permitan erradicar el delito de terrorismo con eficacia.

La crítica habitual que recibe el ‘Derecho penal del enemigo’ es que este modelo desarrolla leyes penales sobre las cuales cabría preguntarse si son “compatibles con el marco constitucional de un Estado de Derecho y con los Pactos internacionales de Derechos civiles reconocidos y acogidos en los ordenamientos jurídicos de los Estados civilizados”⁵³⁰, y en su marco de aplicabilidad, que posee una visión “puramente tecnocrática y funcionalista.”⁵³¹ Por otra parte, es pertinente señalar que el Derecho penal del enemigo es opuesto a los valores democráticos que preconizan las orientaciones de la Unión Europea hacia sus Estados Miembros para que estos desarrollen legislación nacional que permita perseguir los delitos de terrorismo dentro de cada uno de los EEMM, y cooperativamente entre estos, dentro de toda la Unión.

Al respecto, Mariela Morales Antoniazzi introduce una reflexión que nos detiene en la idea de que el desarrollo del Derecho interno de un Estado no debe de ser ajeno o evolucionar de espaldas a la realidad constitucional de la comunidad internacional que lo integra. Así como el nuevo milenio había facilitado el surgimiento de nuevos delitos de origen tecnológico y global, y con ello la necesidad de nuevas tipificaciones, dicho período también ya encontraba

⁵²⁸ *Ibidem*.

⁵²⁹ MUÑOZ CONDE, Francisco (2011): «La generalización del Derecho penal de excepción: tendencias legislativas y doctrinales: entre la tolerancia cero y el Derecho penal del enemigo», *Ciencia Jurídica*, División de Derecho, Política y Gobierno, Universidad de Guanajuato, año 1, N.º 1, p.134.

⁵³⁰ *Ibidem*, p. 135.

⁵³¹ *Ibidem*.

resignificada la posición del Estado dentro del Sistema internacional por lo cual debía dar cuenta de consideraciones constitucionales antes no previstas.⁵³²

Para Morales Antoniazzi:

«La noción de Estado abierto de cuño germánico cuenta con una larga tradición de casi seis décadas y ha sido reinterpretada en este milenio como la permeabilidad del ordenamiento jurídico nacional, con el objeto de significar que el Estado “está vinculado a la comunidad internacional y ello genera transformaciones de su institucionalidad, competencias y en las relaciones internacionales”. En este sentido, es preciso reiterar la vigencia del constitucionalismo de los derechos humanos bajo una perspectiva multinivel que muestra una progresiva y convergente configuración y que subraya que el Estado se somete a la comunidad internacional en pos de un orden jurídico que protege la dignidad humana.»⁵³³

Pensar un Estado actual como un Estado abierto y permeable al sistema constitucional internacional nos hace suponer la existencia, dentro de dicho Estado, de ciertas características democráticas básicas que se encuentran recogidas en la doctrina internacional de los derechos humanos. Es lo que Mariela Morales Antoniazzi denomina como los “estándares mínimos” que todo Estado debe de poseer, por cuanto “la consolidación del Estado constitucional democrático exige estándares mínimos de derechos humanos (identificados en la doctrina constitucional mayoritaria como derechos fundamentales) junto a los estándares de los sistemas universales y regionales de protección de los derechos humanos.”⁵³⁴

Naturalmente, la Política Criminal de un Estado totalitario difiere por completo respecto de la Política Criminal de un Estado de Derecho, como lo son nuestros tres casos de estudio, y en donde son aplicables todas las consideraciones sobre los derechos fundamentales anteriormente mencionadas. Teniendo en consideración esto, cabe preguntarse tal cual lo expresa Francisco Conde Muñoz: “¿Hasta qué punto es legítimo un ‘Derecho penal del enemigo’ que no se atenga a los principios del Estado de Derecho [...]? Y, sobre todo, ¿cuáles son los límites que debe tener el mismo, si es que, por su naturaleza, admite algún tipo de límite?”⁵³⁵

Lo cierto es que, más allá de estas preguntas, la existencia de un Derecho de excepción contemplado en las legislaciones penales de los Estados, y reservado para casos de mayor gravedad que vulneren la seguridad nacional, es una realidad y una tendencia imparable. Alemania no solo habría postulado en su momento la necesidad de poseer un Derecho penal del enemigo para los delitos considerados de terrorismo, sino que también lo ha empleado activamente, y ha acuñado dicha idea en los países que valoran y tradicionalmente siguen la doctrina penal alemana. De tal forma que, las ideas de Jakobs en Alemania han sido con los años las ideas de otros muchos juristas, legisladores y/o parlamentarios de diferentes Estados, europeos y no europeos.

⁵³² De acuerdo con las teorías de las relaciones internacionales, para dicha época (tercer milenio) el Estado ya había dejado de ser un ente aislado y autocrático (según la teoría del realismo político desarrollada por Hans Morgenthau) para convertirse en parte de un sistema global que inevitablemente le expresa e infiere gran influencia. Véase: MORGENTHAU, Hans J. (2020): *Política entre las naciones. La lucha por el poder y la paz*, Santiago de Chile: Ediciones Jurídicas Olejnik.

⁵³³ MORALES ANTONIAZZI, Mariela (2023), «Protección y garantías transnacionales para nuevos y viejos derechos», en: ARAGÓN REYES, Manuel/VALADÉS RÍOS, Diego/TUDELA ARANDA, José, *Derecho Constitucional del Siglo XXI: desafíos y oportunidades*, (129-167), p. 131.

⁵³⁴ *Ibidem*, pp. 132-133.

⁵³⁵ MUÑOZ CONDE, Francisco (2011), *opus cit.*, p. 132.

Teniendo en cuenta entonces que, sí o sí, existe “un ‘Derecho penal del ciudadano’ respetuoso con el Estado de Derecho y un ‘Derecho penal del enemigo’ emanado del poder estatal”,⁵³⁶ una pregunta que parece ser adecuada es la que realiza Juan Antonio García Amado, al expresar: “¿qué hace que una persona pierda su condición de tal y pase a mero individuo?”⁵³⁷ Jakobs es categórico y sintético en su respuesta: “Los enemigos son no-personas.”⁵³⁸ Por lo tanto, no pueden ser tratados como tales. García Amado, explica el pensamiento de Jakobs al respecto de la pérdida de condición de persona:

«Al igual que una norma jurídica perdería su validez al convertirse en ineficaz, la construcción jurídica de la persona decae y el sujeto deja de ser tal y se torna mero individuo cuando incumple de determinada manera o en cierta medida reiterada los deberes jurídicos, o al menos los penales, que le incumben.»⁵³⁹

García Amado, no obstante, posee otra interpretación respecto de esta pérdida de condición de persona, y sugiere que:

«Si la configuración jurídica del sujeto depende de la acción del mismo y no de la adscripción genérica por el Derecho, ya no podrá en propiedad hablarse de que la persona sea un constructo del sistema jurídico mismo, sino, todo lo más, de constructo condicionado a ciertas prestaciones normativas del sujeto mismo. Es decir, no es el Derecho el que hace del individuo persona, sino que persona sería solamente el individuo básicamente obediente.»⁵⁴⁰

En contradicción con Jakobs, para Marc Alexander Zöller el denominado ‘Derecho penal del enemigo’ no es la respuesta. Miguel Ángel Cano Paños, analiza en profundidad la obra de Zöller y detalla la opinión de este autor al expresar que la “existencia de un Derecho penal del enemigo para determinadas constelaciones delictivas (entre ellas, el terrorismo) muestran un enorme potencial de cara al desarrollo de tendencias de Política Criminal equivocadas en el ámbito del Derecho penal tanto sustantivo como procesal.”⁵⁴¹ Según Cano Paños citando a Zöller, “la mera defensa de un Derecho penal del enemigo para delincuentes terroristas supondría para Zöller una victoria de estos últimos sobre la base de su paradigma de confrontación abierta con el Estado destinatario de sus acciones.”⁵⁴²

La aplicación, o no, de un Derecho penal del enemigo, ha suscitado en Alemania innumerables debates que se han trasladado a otros a otros países y hemisferios. Lo cierto es que, en lo concerniente al terrorismo, el común denominador que prevalece es la referencia a un enemigo en común, y a un posicionamiento de lucha por parte de cada Estado, incluso si esto significa la

⁵³⁶ ESER, Albin (2004): «Consideración final», GOMEZ RIVERO, Carmen (Trad.), en: ESER, Albin/HASSEMER, Winfried/BURKHARDT, Björn (Coords.) / MUÑOZ CONDE, Francisco (Coord. versión española), *La ciencia del Derecho penal ante el cambio de milenio*, Valencia: Tirant lo Blanch, (463-476), p. 472.

⁵³⁷ GARCÍA AMADO, Juan Antonio (2006): «El obediente, el enemigo, el Derecho penal y Jakobs», *Nuevo Foro Penal*, enero-junio, No. 69, (100-136), p. 102.

⁵³⁸ Cita original en alemán: “*Feinde sind aktuell Unpersonen*”. Jakobs utiliza el concepto de persona como equivalente a sujeto de derecho. Véase: JAKOBS, Günther (2004), opus cit. p. 60.

⁵³⁹ GARCÍA AMADO, Juan Antonio (2006), opus cit., pp. 102-103.

⁵⁴⁰ *Ibidem*, pp. 102-103.

⁵⁴¹ CANO PAÑOS, Miguel Ángel (2010a): «El Derecho penal ante los desafíos del terrorismo global», *Indret: Revista para el Análisis del Derecho*, N.º 3, (1-32), p.16.

⁵⁴² *Ibidem*, p. 17.

vulneración de las propias garantías constitucionales previamente establecidas en sus constituciones.

Alemania, más que ningún otro país, ha desarrollado una propia lucha interna que se ha caracterizado por el delicado equilibrio entre la erradicación de toda forma de extremismo violento y el mantenimiento de los derechos fundamentales. Se podría decir, sin lugar duda, que es esta relación de autocontrol constitucional lo que ha caracterizado a la Política Criminal alemana en su lucha contra el terrorismo. Ello ha significado que Alemania siempre ha priorizado el desarrollo de una lucha contra el terrorismo dentro de la ley.

Probablemente, este hecho de permanente autocontrol orientado a no vulnerar su propia constitución ha logrado que Alemania desarrolle como ningún otro país de la Unión Europea, todo tipo de medidas preventivas, incluyendo grandes inversiones de presupuesto, para eliminar los factores originarios que detonan los radicalismos dentro de su frontera. Ello indica que Alemania previene antes de que los actos terroristas tengan lugar.

Con relación a este enfoque, resulta interesante el hecho de que Alemania se refiera al terrorismo como extremismo violento. El extremismo violento no implica necesariamente la acción delictiva, puede describir solo una ideología, un modo de vivir o de sentir respecto a algo. Por el contrario, el terrorismo siempre lleva aparejado la acción violenta, el atentado, el acto, el ataque. No se es terrorista con el pensamiento, se es extremista con el pensamiento.

En consecuencia, no es de extrañar el hecho de que Alemania libre su lucha, tal como lo describe en su normativa e informes públicos, contra toda forma de extremismo violento (no terrorismo), porque busca posicionar sus medidas principalmente en el marco de la prevención, es decir, antes de la comisión delictiva.

Este modelo de Política Criminal, aunado al control constitucional que realiza Alemania sobre su legislación, es propio del *lawfare*, y orienta al Estado a llevar adelante una ‘guerra legal’ contra el extremismo violento, en un ejercicio de máxima autorreflexión crítica.⁵⁴³

⁵⁴³ El Gral. Charles Dunlap fue quien introdujo en el año 2001 en concepto de *lawfare*, el cual se resume sintéticamente como “*el uso de la ley como arma de guerra*”. El *lawfare*, para Dunlap, es “*simplemente otro tipo de arma, una que se produce*” [...] “*convirtiendo los libros de derecho en espadas*”. Véase: DUNLAP, Charles J. Jr. (2001): «Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts», *Working Paper*, Carr Center for Human Rights, John F. Kennedy, Harvard.

Según Melissa Waters el concepto de *lawfare* se ha desvirtuado con los años, principalmente mediante utilizaciones controvertidas por parte del entonces presidente Bush, cuando presentó su Estrategia de Seguridad Nacional en el año 2002. Para Melissa Waters “*es evidente que la ‘guerra legal’, en la guerra contra el terrorismo, se ha desviado considerablemente de sus raíces no partidistas e ideológicamente neutrales.*” Para consolidar esta afirmación, Waters cita a Scott Horton quien sostiene que “*el término fue secuestrado por la derecha, y se convirtió en una herramienta, en un derbi de demolición legal*” y, que por lo tanto, este concepto ha quedado “*irremediabilmente desacreditado.*” Melissa Waters rescata el sentido original del concepto de Dunlap, y recuerda que “*Dunlap se refería a restaurar la justicia por medio de la lucha legal*”. Pero Waters reflexiona, y se pregunta: “*¿Se puede recuperar la ‘guerra legal’ de manos de los expertos políticos y (re)desarrollarla hasta convertirla en un concepto útil para los estrategas militares y legales en la conducción de la guerra contra el terrorismo?*” [...] El *lawfare* “*contempla el uso del derecho y los procesos legales como instrumento de guerra, pero no se centra exclusivamente en esta definición estrecha, sino que abarca una discusión más amplia sobre el papel adecuado del derecho en la gestión de la guerra.*” [...] “*La concepción de ‘autorreflexión crítica’ del lawfare reconoce el hecho (que Dunlap ha enfatizado repetidamente en su reciente escritos) de que la ley es simplemente un instrumento de guerra neutral, que puede ser utilizado por todos los bandos en la guerra contra el terrorismo.*” Véase: WATERS, Melissa A. (2010): «‘Lawfare’ in the War on Terrorism: A Reclamation Project», *Case Western Reserve Journal of International Law*, Volume 43, Issue 1, (327-334), pp. 327-331.

LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL ALEMANA

INSTRUMENTOS NORMATIVOS PARA LA PERSECUCIÓN DEL TERRORISMO ONLINE

En los inicios de su lucha contra el terrorismo local, Alemania decidió que no crearía ninguna legislación especial para tratar de forma este tipo de delito. Debido a ello, el Estado alemán desarrolla, desde una perspectiva legislativa, su lucha contra el terrorismo mediante las herramientas normativas tradicionales de las que dispone y que se encuentran dentro de su Derecho penal común.⁵⁴⁴

Ello significa que no existe el delito de terrorismo como tal, sino la punición de las múltiples manifestaciones violentas que cualquier extremismo puede tener. Esta falta de legislación específica en la materia no significa que Alemania no conceda importancia a la lucha contra el terrorismo. Por el contrario, la lucha contra el terrorismo posee especial atención dentro de su Política Criminal y, se fomenta que el Estado sostenga esta lucha mediante el enjuiciamiento penal eficaz apegado a los estándares del Estado de Derecho.

La pugna que ha tenido lugar dentro de la doctrina penal alemana entre la aplicación del Derecho penal ciudadano (general) y el ‘Derecho penal del enemigo’, ha sido tal que se ha incentivado el hecho de que los actos terroristas individuales son perseguidos por medio de las disposiciones de la legislación penal general.⁵⁴⁵

Sin embargo, luego de los atentados del 11-S en el año 2001 y con los incipientes atentados terroristas yihadistas en Europa, Alemania comenzó a incorporar una serie de disposiciones normativas que fueron dando forma a su actual legislación en la materia.

Bajo esta tendencia, tuvo lugar, en agosto del año 2009, la incorporación de tres disposiciones en el Código Penal alemán mediante la adopción de la *Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten* (GVVG)⁵⁴⁶ que poseen relación directa con el terrorismo. Las nuevas disposiciones penales tipifican los actos preparatorios del delito, en los actos considerados violentos y graves que pongan en peligro al Estado (Sección 89ª del Código Penal), a su vez penalizan el inicio o mantenimiento de contactos con una organización terrorista con finalidad delictiva (Sección 89b del Código Penal), y la distribución de instrucciones para cometer un acto violento grave que ponga en peligro al Estado (Sección 91 del Código Penal). En junio de 2015, las secciones 89a y 89b del Código Penal fueron modificadas nuevamente por medio de la *Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten* (GVVG-ÄndG).⁵⁴⁷ Dicha enmienda busca incluir en la tipificación los viajes realizados al extranjero⁵⁴⁸ con la intención de recibir instrucción militar y

⁵⁴⁴ Código Penal alemán (*Strafgesetzbuch*). Disponible en: www.gesetze-im-internet.de [Fecha de consulta: 26 de noviembre de 2023].

⁵⁴⁵ Por regla general, las tipificaciones de aplicabilidad más recurrentes son el homicidio y las lesiones corporales, los delitos contra la libertad personal, los delitos contra el orden público y los delitos peligrosos para la población (incendio provocado, creación de explosión y envenenamiento).

⁵⁴⁶ Ley sobre el Procesamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado.

⁵⁴⁷ Ley de Enmienda sobre el Enjuiciamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado.

⁵⁴⁸ Principalmente a Libia, Siria, Irak y Turquía.

adoctrinamiento, y debido a ello, posteriormente al retorno, facilitar los actos de terrorismo en el territorio alemán. Esta nueva tipificación busca estar en consonancia con las medidas recogidas en la Resolución 2178 (2014)⁵⁴⁹, de 24 de septiembre de 2014, adoptadas por el Consejo de Seguridad de las Naciones Unidas, en donde se aborda las amenazas específicas que plantean los combatientes terroristas extranjeros.

Cabe señalar que en la adopción de esta enmienda se introdujo también la figura de financiación del terrorismo mediante su tipificación en la Sección 89c del Código Penal, debido a que Alemania interpreta que las organizaciones terroristas como Estado Islámico posee sobrados recursos financieros para apoyar y promover dichos viajes y actividades terroristas.

Respecto a la tipificación adoptada en la sección 89a, sobre la preparación de un acto violento grave que ponga en peligro al Estado, se entiende que se incurre en el mismo bajo las siguientes circunstancias:

«(1) Quien prepare un delito violento grave que ponga en peligro al Estado incurre en una pena de prisión de seis meses a diez años. Un "delito violento grave que pone en peligro al Estado" significa un delito contra la vida en los casos previstos en los artículos 211 o 212 o contra la libertad personal en los casos previstos en los artículos 239a o 239b que, dadas las circunstancias, tiene por objeto y es adecuado socavar la existencia continuada o seguridad de un Estado o de una organización internacional, o para abolir, privar de efecto jurídico o subvertir los principios constitucionales de la República Federal de Alemania.

(2) La subsección (1) sólo se aplica a los delincuentes que preparan un delito violento grave que pone en peligro al Estado al

1. instruir a otra persona o recibir instrucción sobre la producción o el uso de armas de fuego, explosivos, dispositivos explosivos o incendiarios, materiales de fisión nuclear u otras sustancias radiactivas, sustancias que contengan o puedan producir veneno, otras sustancias nocivas para la salud, dispositivos especiales que sean necesarios para la comisión del delito u otras habilidades que puedan ser útiles en la comisión de un delito previsto en el apartado (1),

2. producir, obtener para sí o para otro, almacenar o suministrar a otro armas, sustancias o artefactos a que se refiere el n. 1

3. obtener o almacenar objetos o sustancias esenciales para la producción de armas, sustancias o dispositivos a que se refiere el n. 1.»⁵⁵⁰

En las nuevas disposiciones penales existen unas alusiones directas al uso de Internet por parte de los grupos terroristas yihadistas. Con relación a la financiación del terrorismo, se enuncia que es requerida la vigilancia y el registro de las telecomunicaciones de conformidad con el sección 100a del Código de Procedimiento Penal, dado que se entiende que la preparación y financiación de actos terroristas se lleva a cabo habitualmente de forma aislada, utilizando medios de comunicación modernos.

Por otra parte, en la sección 91, referida al delito que supone fomentar la comisión de un delito violento grave que ponga en peligro al Estado, abarca la difusión y promoción de contenido yihadista propagandista que aliente y/o sirva de orientación para la comisión de un delito

⁵⁴⁹ La S/RES/2178 (2014) “prevé que los viajes o los intentos de viajar a un Estado que no sea el de residencia o nacionalidad de la persona que viaja sean procesados en una forma apropiada a la gravedad del delito si el viaje tiene como objetivo llevar a cabo actos terroristas para cometer, planificar, preparar o participar en o entrenar terroristas o ser entrenado como terroristas.” Véase: *Entwurf eines Gesetzes zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten* (GVVG-Änderungsgesetz - GVVG-ÄndG), vom 05.02.2015, p. 1.

⁵⁵⁰ Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906). Véase: Section 89a “Preparation of serious violent offence endangering state.”

violento grave que ponga en peligro al Estado. Sí bien no se detallan los medios por los que se debe llevar a cabo esa difusión y propaganda, la disposición es perfectamente adoptable para los actuales usos de Internet por parte del terrorismo. Sin embargo,

«[...] el nuevo § 91 StGB constituye en esencia un instrumento de dudosa eficacia para afrontar la delincuencia de carácter terrorista. Sin ir más lejos, el párrafo segundo núm. 2 de dicha disposición exige un elemento subjetivo del tipo adicional al dolo, consistente básicamente en la intención del autor de cometer un delito violento grave contra la seguridad del Estado. Es evidente que este propósito adicional será generalmente difícil de demostrar durante del proceso penal que se siga por ejemplo contra un sujeto que tiene almacenado en su ordenador un manual de instrucciones para la fabricación de una bomba.»⁵⁵¹

Considerando la amplia usabilidad que posee Internet para la comisión delictiva terrorista, se prevén diversos usos y se recoge en diversas disposiciones las penas previstas para “quien apoye una organización terrorista tal como se define en el Código Penal” (según sección 129a y subsecciones (1) y (2) del Código Penal), o reclute miembros o partidarios de dicha organización será castigado con penas de prisión de seis meses a cinco años.” (De acuerdo con la sección 129a y subsección (5), párrafos 1 y 2 del Código Penal). Con ello se pretende evitar la propaganda online del yihadismo con fines de incitación al terrorismo, radicalización y reclutamiento que suele alojarse en sitios webs de dominio adquirido propio o diversas redes sociales y se consultado por simpatizantes del yihadismo. Conforme al párrafo 1, y de acuerdo con Miguel Ángel Cano Paños, estaría sujeto a responsabilidad penal,

«[...] aquel sujeto que elogia o hace accesible a otro un escrito o publicación, el cual por su contenido resulta apropiado para servir como instrucción para un delito violento grave contra la seguridad del Estado. Para ello resulta necesario que las circunstancias en las que se lleva a cabo esa difusión resulten proclives para despertar o fomentar la disposición de otros sujetos a llevar a cabo dicha acción delictiva. Lo mismo cabe decir con respecto a aquel sujeto que se hace con un escrito o publicación idóneo para servir como instrucción para cometer un delito violento grave contra la seguridad del Estado, siendo en este caso suficiente para afirmar la tipicidad de la conducta que el autor almacene en su ordenador o en un servidor externo la información obtenida.»⁵⁵²

Miguel Ángel Cano Paños, citando a Zöller, detalla que también “los proveedores de estas páginas, a través de la cuales se pueden llevar [...] actividades de reclutamiento y recaudación de fondos, pueden verse sometidos a una persecución penal sobre la base de los párrafos § 129a y § 129b StGB.”⁵⁵³

El Derecho penal alemán faculta, en caso de delitos graves, a establecer métodos de investigación que posibilitan la interceptación de las telecomunicaciones del acusado, incluso a través de comunicaciones móviles, fax, correo electrónico e Internet; y podrá ordenarse mediante orden judicial por una duración máxima de tres meses (Secciones 100a y siguientes del Código de Procedimiento Penal). En caso de que las investigaciones duren más de tres meses se requiere una aprobación mediante una renovación judicial. Bajo estas condiciones previas, también está permitido interceptar equipos de telecomunicaciones de terceros si se puede suponer que estas personas actúan como mensajeros del acusado. Además de la recopilación de datos de tráfico, sobre la base de una sentencia judicial, también se puede recopilar la ubicación

⁵⁵¹ CANO PAÑOS, Miguel Ángel (2010a), opus cit., p. 20

⁵⁵² *Ibidem*.

⁵⁵³ *Ibidem*.

de un teléfono móvil y los detalles del respectivo terminal móvil o número de tarjeta (Secciones 100g a 100i del Código de Procedimiento Penal). Como último recurso, también sobre la base de una orden judicial, la vida privada del acusado también puede ser interceptada y grabada dentro y fuera de ámbitos privados, oficinas y locales comerciales de acceso general (Sección 100c, subsección (1) N.º 2 y 3 del Código de Procedimiento Penal).

El Código Penal alemán prevé que en general siempre todas las partes interesadas deben ser informadas posteriormente de la implementación de medidas de vigilancia de sobre las comunicaciones y/o utilización de otros métodos de investigación encubiertos (Sección 101 del Código de Procedimiento Penal).

Para la implementación efectiva de estas medidas de investigación, la legislación contempla que se podrán utilizar “ayudas técnicas especiales en el contexto de la observación planificada relacionada con delitos de importancia sustancial, como equipos de visión nocturna, sistemas de seguimiento y el Sistema de Posicionamiento Global (GPS) guiado por satélite”. Además, se pueden tomar fotografías y realizar grabaciones visuales fuera de las instalaciones (Sección 100h, subsección (1) N.º 1 y 2 del Código de Procedimiento Penal).

Las secciones 102 y 103 permiten un “registro de los locales privados y de otro tipo del sospechoso, que en principio debe ser ordenado por un juez, salvo en casos de circunstancias apremiantes, cuando se pueda presumir que ello conducirá al descubrimiento de pruebas específicas” (Sección 102 del Código de Procedimiento Penal). Los registros hacia otras personas están justificados si existen ciertos hechos que sugieran que la persona que se va a detener, o la prueba específica que se busca, se encuentra dentro de sus instalaciones (Sección 103 del Código de Procedimiento Penal).

Los agentes de policía con una identidad modificada (agente encubierto) pueden ser “desplegados como investigadores encubiertos para resolver delitos de importancia sustancial” (Sección 110a y siguientes del Código de Procedimiento Penal). En este contexto, personas pueden apoyar a las autoridades de investigación revelando información de la que hayan tenido conocimiento a cambio de una garantía de confidencialidad. En el marco de las investigaciones, “todo rastro encontrado en la escena del crimen puede ser examinado utilizando métodos moleculares y genéticos y ser comparado con ADN almacenado del sospechoso” (Secciones 81a, 81e y 81g del Código de Procedimiento Penal). Además, para investigar y procesar delitos terroristas, “se puede realizar una comparación de datos automatizada para verificar ciertas características manifestadas por el delincuente” (Sección 98a del Código de Procedimiento Penal). Para lograr el cometido de llevar adelante una investigación utilizando métodos genéticos, “se pueden establecer puntos de control en lugares de acceso público” (Sección 111 del Código de Procedimiento Penal).

La Política Criminal alemana orientada con relación al terrorismo no busca sostener una lucha contra esta forma de delincuencia únicamente por la vía normativa, sino que orienta también sus esfuerzos a otras formas de prevención. Es decir, Alemania aplica dentro de su Política Criminal lo que Peter Lejins denomina prevención punitiva por medio del Derecho penal, pero no

descuida en absoluto la aplicación de la prevención mecánica y prevención orgánica que detalla este autor.⁵⁵⁴

No obstante, aun cuando las otras formas preventivas, que se estudiarán a continuación otorgan gran resultado, para Marc Alexander Zöller de acuerdo con Miguel Ángel Cano Paños, el Derecho penal constituiría “el único instrumento reactivo que se encuentra en disposición de contrarrestar la violencia terrorista” Para este autor, “los aspectos de prevención general y especial [...] únicamente pueden desplegar una eficacia limitada con respecto a aquellos delincuentes que han sufrido un proceso de adoctrinamiento de carácter político, religioso o en general ideológico,”⁵⁵⁵ debido principalmente porque los terroristas son incapaces de legitimar la autoridad del Estado y reconocer las competencias del mismo.

MEDIDAS DE CONTROL Y VIGILANCIA, Y REPRESIÓN CONTRA EL YIHADISMO EN INTERNET

Después del 11 de septiembre de 2001, Alemania procedió a una ampliación selectiva de las estructuras de seguridad utilizando una serie de amplias medidas legales, operativas y administrativas, y se promovió una coordinación cuidadosamente entre sí de todas las medidas reglamentarias, operativas y preventivas.

Se desarrollaron dos paquetes de seguridad (*Sicherheitspakete*)⁵⁵⁶ que tendieron a la mejora de desarrollar investigaciones y esclarecer las intenciones delictivas en el período previo a las actividades antiterroristas. De esta forma, entre otras áreas de aplicación, se obtuvo información valiosa sobre los movimientos de viaje realizados por sujetos sospechosos, flujos financieros y/o los cambios de identidad que realizan los sujetos sospechosos a su retorno a Europa. Por otra parte, en la misma línea de identificación de retornados, se ha conseguido establecer mejoras en materia de seguridad aeroportuaria.

El Paquete de Seguridad N.º 1, aprobado el 9 de noviembre y en vigor desde el 8 de diciembre de 2001, permite ampliar las actuaciones a fin de imponer prohibiciones a las comunidades religiosas y sociedades filosóficas extremistas teniendo por base legal lo recogido en la Ley de Asociaciones. Dicha Ley de Asociaciones, facultaría la prohibición cuando la asociación a comunidades religiosas y sociedades filosóficas “[...] cuyos fines o cuya actividad sean contrarios a las leyes penales o que estén dirigidas contra el orden constitucional o contra la idea del entendimiento entre los pueblos.”⁵⁵⁷

Con esta medida se elimina el ‘privilegio religioso’, que hasta entonces había sido aplicable y conforme al cual las restricciones impuestas por la Ley de Asociaciones a otras agrupaciones no poseían efecto alguno en las comunidades religiosas. A partir de esta medida, varias organizaciones fueron prohibidas en Alemania, entre ellas el ‘Estado Califal’ (prohibida el 8 de diciembre de 2001), y también ‘*Al-Aqsa e.V.*’ y ‘*Hizb ut-Tahrir*’ (ambas prohibidas en Alemania

⁵⁵⁴ Este tipo de orientaciones preventivas son parte de la calificación de Peter Lejins. De acuerdo con el autor los modelos aplicados pueden determinar una prevención punitiva, una prevención correctiva o una prevención mecánica. Véase: VIRGINIA DEPARTMENT OF CRIMINAL JUSTICE SERVICES (2018), opus cit., pp. 28-31.

⁵⁵⁵ CANO PAÑOS, Miguel Ángel (2010a), opus cit., p. 14.

⁵⁵⁶ CANO PAÑOS, Miguel Ángel (2008c): «Respuestas legales al terrorismo yihadista. El ejemplo de Alemania», Athena Intelligence Journal, Vol. 3, N.º 1, (45-77), p. 48.

⁵⁵⁷ Ley Fundamental de la República Federal de Alemania (*Grundgesetz*). Libertad de asociación, artículo 9.2.

el 15 de enero de 2003). Años más tarde, concretamente en el 2020, se prohíbe la organización ‘Hezbollah’.⁵⁵⁸

El Paquete de Seguridad N.º 2, entró en vigor el 1 de enero de 2002, y con el mismo se adopta, el 9 de enero de 2002, la Ley de Lucha contra el Terrorismo Internacional (*Gesetz zur Bekämpfung des internationalen Terrorismus, Terrorismusbekämpfungsgesetz*, TBG), por medio de la cual se adaptaron muchas leyes de seguridad y otras leyes de diversos ámbitos ante la nueva amenaza del yihadismo.

A partir de la adopción de estos dos paquetes de seguridad, tuvo lugar una serie de cambios que se reflejaron en la Ley Federal de Protección Constitucional⁵⁵⁹, la Ley del Servicio de Contrainteligencia Militar⁵⁶⁰, la Ley del Servicio Federal de Inteligencia⁵⁶¹, la Ley de la Policía Federal [Frontera]⁵⁶², la Ley de la Oficina Federal de Policía Criminal⁵⁶³, así también como en normas relativas a extranjería. Todo ello ha permitido mejorar la comunicación entre autoridades y agilizar la información compartida, impedir la entrada de extremistas a territorio alemán, e identificar a aquellos que ya han tenido su entrada al país.

Además, la Ley de Control de Seguridad⁵⁶⁴, la Ley de Pasaportes⁵⁶⁵, la Ley de Cédulas de Identidad⁵⁶⁶, la Ley de Asociaciones⁵⁶⁷, la Ley de Aviación Civil⁵⁶⁸, la Ley del Registro Central

⁵⁵⁸ «Alemania prohíbe toda actividad del grupo terrorista libanés Hezbollah», *El periódico de Aragón*, edición online de 30 de abril de 2020. Disponible en: <https://www.elperiodicodearagon.com/internacional/2020/04/30/alemania-prohibe-actividad-grupo-terrorista-46536814.html> [Fecha de consulta: 29 de noviembre de 2023].

⁵⁵⁹ Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 1 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 413) geändert worden ist. (Ley Federal de Protección Constitucional de 20 de diciembre de 1990 (BGBl. I p. 2954, 2970), modificada por última vez por el artículo 1 de la Ley de 22 de diciembre de 2023 (BGBl. 2023 I No. 413)).

⁵⁶⁰ Gesetz über den militärischen Abschirmdienst (MAD-Gesetz - MADG). (Ley del Servicio de Contrainteligencia Militar).

⁵⁶¹ Significó que se establecieran cambios a la Ley Federal de Protección Constitucional, la Ley del Servicio Federal de Inteligencia y la Ley del Servicio de Contrainteligencia Militar. A partir de esta adopción las tres agencias gubernamentales: La Oficina Federal para la Protección de la Constitución, el Servicio Federal de Inteligencia y el Servicio de Contrainteligencia Militar tienen derecho a solicitar información sobre los datos de las conexiones de telecomunicaciones y los datos sobre los teleservicios utilizados. Por su parte también, la Oficina Federal para la Protección de la Constitución y el Servicio Federal de Inteligencia tienen derecho a solicitar información a los bancos sobre transferencias de dinero e inversiones. Y en una expresión de mayor competencia, la Oficina Federal para la Protección de la Constitución también tiene derecho a solicitar a los operadores aéreos información sobre los nombres, direcciones y servicios de transporte utilizados, y a solicitar información a los operadores postales. Véase: Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) (Ley del Servicio Federal de Inteligencia). Última modificación: *BND-Gesetz vom 20. Dezember 1990* (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 1 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 410) geändert worden ist, (Ley del BND de 20 de diciembre de 1990 (BGBl. I p. 2954, 2979), modificada por última vez por el artículo 1 de la ley de 22 de diciembre de 2023 (BGBl. 2023 I No. 410)).

⁵⁶² “Se ha introducido la posibilidad de desplegar agentes de la Policía Federal [Frontera] para garantizar y restablecer la seguridad a bordo de los aviones alemanes”. Véase: Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG) § 2 Grenzschutz (Ley de la Policía Federal, BPolG. Artículo 2 Protección de fronteras).

⁵⁶³ “Cambios a la Ley de la Oficina Federal de Policía Criminal: Ampliación de la competencia de investigación original de la Oficina Federal de Policía Criminal para incluir determinados casos graves de delitos relacionados con redes de datos (ciberdelito); [y] Fortalecimiento de la competencia de la Oficina Federal de Policía Criminal como sede tanto de la administración federal como de los Länder federales ampliando su autorización para obtener datos”. Véase: Bundeskriminalamtgesetz (Ley de la Oficina Federal de Policía Criminal).

⁵⁶⁴ Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen, Sicherheitsüberprüfungsgesetz - SÜG) (Ley sobre los requisitos y el procedimiento para los controles federales de seguridad y la protección de información clasificada, Ley de Control de Seguridad - SÜG).

⁵⁶⁵ Paßgesetz, PaßG (Ley de pasaportes, PassG).

⁵⁶⁶ Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG). Ley sobre cédulas de identidad y prueba electrónica de identidad (Ley de cédulas de identidad - PAuswG)

⁵⁶⁷ Gesetz zur Regelung des öffentlichen Vereinsrechts (Vereinsgesetz). Ley que regula el derecho de asociaciones públicas (Ley de Asociaciones)

⁵⁶⁸ Luftverkehrsgesetz (LuftVG). Ley de aviación (LuftVG).

Federal⁵⁶⁹, y el Libro Décimo del Código Social (Libro X)⁵⁷⁰, se modificaron también con el objeto de facilitar los controles de seguridad sobre personas empleadas en instalaciones esenciales para la defensa nacional, incorporar características biométricas en pasaportes y documentos de identidad, otorgar el derecho de utilizar armas en aeronaves civiles a los agentes de policía, poder actuar más rápidamente en las detenciones de grupos extremistas de extranjeros en Alemania, y mejorar la comparación automatizada de datos (*Rasterfahndung*).

Todas estas medidas de carácter operativo han ido incorporándose paulatinamente a la Política Criminal de Alemania, y han ido configurando su estrategia frente al terrorismo internacional que nació posteriormente al 11-S. Para Miguel Ángel Cano Paños, “testigos directos de esta estrategia son la Ley de Lucha contra el Terrorismo Internacional (*Terrorismusbekämpfungsgesetz*), de 9 de enero de 2002, así como la Ley Complementaria de la Ley de Lucha contra el Terrorismo, aprobada el 5 de enero de 2007.”⁵⁷¹

En 2009, concretamente el 1 de enero de 2009, entraron en vigor las enmiendas a la Ley de la Oficina Federal de Policía Criminal (*Bundeskriminalamtgesetz*), lo que significó un hecho crucial dentro de la seguridad de Alemania. A partir de dicho cambio legislativo, la Oficina Federal de Policía Criminal (*Bundeskriminalamt*, BKA) obtuvo mayores facultades para luchar contra la amenaza del terrorismo internacional. Estas facultades apoyan en gran medida modelos acción policial cuya base se encuentra en la Ley Federal de Policía (*Bundespolizeigesetz*) y en las leyes policiales estatales, estas últimas otorgan potestad a las Oficinas de Policía Criminal del Land (*Landeskriminalämter*, LKA).

La Oficina Federal de Policía Criminal (*Bundeskriminalamt*, BKA) con base en la nueva ley ha podido organizar sus tareas bajo una nueva estructura que actualmente desarrolla en tres niveles:

- «Aumento de la presión para hacer cumplir la ley y desarrollo del instrumento de evaluación de riesgos “RADAR-rechts” (primer nivel).
- Identificar redes de forma más rápida y eficiente (segundo nivel).
- Luchar contra los delitos de odio en línea con el establecimiento de una Unidad Central de Denuncia de Contenidos Delictivos en Internet (tercer nivel).»⁵⁷²

Desde un punto de vista de su aplicabilidad, ello significa, por ejemplo, el acceso remoto por parte de autoridades policiales a un ordenador de una persona sospechosa de actividades terroristas facultaría a la Oficina Federal de Policía Criminal, por medio del artículo 20k de la Ley Federal de Policía Criminal, a recopilar datos de los sistemas de información a través de medios técnicos o softwares específicos, con el fin de evitar amenazas terroristas y prevenir determinados delitos penales.

Un control de constitucionalidad posterior validó el uso de tales medidas, por lo tanto, la Oficina Federal de Policía Criminal hoy en día sigue utilizando herramientas tecnológicas para contrarrestar el uso de las TIC por parte de los terroristas.

⁵⁶⁹ *Bundeszentralregistergesetz (BZRG)*. Ley del Registro Central Federal (BZRG).

⁵⁷⁰ *Zehntes Buch Sozialgesetzbuch, Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X)*. Libro Décimo del Código Social, Procedimientos Administrativos Sociales y Protección de Datos Sociales (SGB X).

⁵⁷¹ CANO PAÑOS, Miguel Ángel (2010a), opus cit., p. 2.

⁵⁷² US DEPARTMENT OF STATE. Country Reports on Terrorism 2020: Germany. Disponible en: <https://www.state.gov/reports/country-reports-on-terrorism-2020/germany/> [Fecha de consulta: 29 de noviembre de 2023].

Una vez concluidas y presentadas las investigaciones policiales, las institucionales jurídicas que intervienen en el procesamiento de las acciones de terrorismo son el Fiscal General Federal (*Generalbundesanwalt*, GBA), los Tribunales Regionales Superiores (*Oberlandesgerichte*, OLG), y el Tribunal Federal de Justicia (*Bundesgerichtshof*, BGH), y cuentan en el desarrollo de su labor con el apoyo permanente de la Oficina Federal de Policía Criminal, las Oficinas de Policía Criminal del Land y la Policía Federal (*Bundespolizei*, BPol) también ejercen funciones preventivas en el marco de la lucha contra el terrorismo.

Los servicios de inteligencia poseen una labor determinante en las investigaciones policiales en materia de terrorismo. Entre ellas se encuentran el Servicio Federal de Inteligencia (*Bundesnachrichtendienst*, BND), que es responsable de la adquisición de información en el extranjero, la Oficina Federal para la Protección de la Constitución (*Bundesamt für Verfassungsschutz*, BfV) y el Servicio de Contrainteligencia Militar (*Militärischer Abschirmdienst*, MAD). como servicios de inteligencia nacionales.

En investigaciones en donde se constaten delitos derivados de acciones de financiación de terrorismo también interviene la Autoridad Federal de Supervisión Financiera (*Bundesanstalt für Finanzdienstleistungsaufsicht*, BaFin), así como la Unidad de Inteligencia Financiera (*Zentralstelle für Verdachtsanzeigen*). Ambas son responsables de llevar adelante acciones prioritarias en el ámbito de la represión de la financiación del terrorismo.⁵⁷³

El Estado alemán cuenta con una fuerte estructura institucional para la represión del delito de terrorismo y que se desempeña al amparo de una legislación que constantemente se revisa en cuanto a su desempeño constitucional.

Todas estas medidas de carácter institucional en donde la cooperación entre las partes resulta fundamental han robustecido, según Miguel Ángel Cano Paños, “las competencias de vigilancia e intervención de los servicios de inteligencia y las fuerzas de seguridad con finalidades tanto preventivas como de persecución penal.”⁵⁷⁴

En el año 2015 se mejora la cooperación precisamente en el ámbito de la inteligencia nacional. Dichas mejoras habían sido introducidas inicialmente de forma temporal después de 11 de septiembre de 2001, pero tras su ampliación hasta enero de 2021, continua su utilización mediante una ley específica. La Ley para Mejorar el Intercambio de Información en la Lucha contra el Terrorismo Internacional⁵⁷⁵ entró en vigor el 30 de julio de 2016, y permite crear bases de datos conjuntas con otros EEMM de la Unión Europea y con terceros Estados, a fin de colaborar con los principales servicios de inteligencia extranjeros, y. facilitar el intercambio de información.

En el fomento de esta cooperación internacional Alemania se ha comprometido en dos aspectos concretos, por un lado, a colaborar con el ámbito de la extradición y la asistencia mutua y, por otro, a ser miembro activo en las Organizaciones Internacionales dedicadas a la lucha contra el terrorismo.⁵⁷⁶

⁵⁷³ FUENTES I GASÓ, Josep Ramon (2017): «El régimen jurídico de prevención de peligros en Alemania: La vigencia de un modelo histórico», *Revista Aragonesa de Administración Pública*, núm. 49-50, Zaragoza, pp. 26-86.

⁵⁷⁴ CANO PAÑOS, Miguel Ángel (2010a), opus cit., p. 2.

⁵⁷⁵ *Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus*, G.v. (Boletín Oficial Federal I, 26 de julio de 2016, página 1818 (N.º 37); Válido a partir del 30 de julio de 2016).

⁵⁷⁶ Unión Europea (UE), Grupo de Acción Financiera Internacional (FATF), OTAN, G7 Roma/Lyon, ONU.

En el ámbito de la Unión Europea, cabe señalar que Alemania ha tenido un protagonismo en cuanto a las acciones de cooperación mutua en materia de seguridad y defensa, y en las orientaciones específicas de la Política Común de Seguridad y Defensa de la Unión. Es reseñable el hecho de que los Estados Miembros hayan adoptado “por primera vez por unanimidad un documento estratégico: la Brújula Estratégica [cuya implementación] es el resultado de una iniciativa alemana” durante la Presidencia del Consejo de Alemania en 2020.⁵⁷⁷

MEDIDAS PREVENTIVAS Y CAMPAÑAS DE INFORMACIÓN

Con el objeto de combatir las causas del terrorismo, el Gobierno alemán ha adoptado también otro tipo de medidas tendientes a promover un debate intelectual y político sobre el extremismo violento, y, aunque ha desarrollado sus bases preventivas sobre otras formas de extremismo violento, se ha centrado en particular sobre el extremismo del fundamentalismo islámico. Estas medidas de carácter orgánico⁵⁷⁸ están orientadas al logro de una prevención exitosa dentro de los estándares del Estado de Derecho. En Alemania no se utilizan los términos CVE (CEV) o PVE (PEV), no obstante, las medidas preventivas que desarrolla el país “se pueden atribuir correctamente a estos conceptos en el sentido de que se basan en prevenir la participación en el extremismo o contrarrestar su crecimiento, en lugar de limitarse únicamente a respuestas represivas a incidentes extremistas o terroristas.”⁵⁷⁹

Dichas medidas, conocidas internacionalmente como Prevenir el Extremismo Violento (PEV) y Combatir el Extremismo Violento (CEV), han tenido un amplio desarrollo dentro del Estado alemán⁵⁸⁰, debido principalmente al hecho de que Alemania siempre ha considerado la prevención del terrorismo por medio de vías alternativas a la punición del Derecho penal. Todo ello ha llevado a que Alemania sea uno de los Estados Miembros de la Unión Europea que mayor utilización ha hecho de estas medidas de carácter no coercitivo, y que, por tanto, sin lugar a duda posee una gran experiencia y se posiciona como un referente en esta modalidad preventiva.

Antes de gozar del desarrollo que posee actualmente este modelo preventivo caracterizado por medidas de P/CEV, cabe señalar que inicialmente las acciones preventivas orientadas a la lucha contra el extremismo violento en Alemania recaían en los servicios de inteligencia federales y estatales (Verfassungsschutz) y en las agencias policiales federales y locales.⁵⁸¹

En el año 2004 se creó, en Berlín, el Centro Conjunto Contra el Terrorismo (*Gemeinsames Terrorismusabwehrzentrum*, GTAZ). El GTAZ es una plataforma de cooperación que utilizan todas las agencias de Alemania que se encargan de luchar contra el terrorismo dentro del territorio. Por medio de GTAZ se comunican los servicios de inteligencia nacionales y extranjeros, la Oficina Federal de Policía Criminal (BKA) y la Procuraduría General de la

⁵⁷⁷ FEDERAL MINISTRY OF DEFENCE (2022): National Security Strategy, Germany. Strategic Concept 2022. Disponible en: <https://www.bmvg.de/en/national-security-policy> [Fecha de consulta: 29 de noviembre de 2023].

⁵⁷⁸ VIRGINIA DEPARTMENT OF CRIMINAL JUSTICE SERVICES (2018), opus cit.

⁵⁷⁹ SAID, Behnam T./FOUAD, Hazim (2018): «Countering Islamist Radicalisation in Germany: A Guide to Germany’s Growing Prevention Infrastructure», *ICCT Policy Brief*, September, International Centre for Counter-Terrorism-The Hague, (1-17), p. 1.

⁵⁸⁰ Alemania lleva implementando, dentro de su territorio, medidas de P/CEV desde hace más de 30 años para disminuir los actos de extremismo violento en su territorio. En primera instancia se orientó al terrorismo de izquierda (RAF), y posteriormente al terrorismo yihadista y luego al extremismo violento de extrema derecha. Véase: KOEHLER, Daniel (2021), opus cit., pp. 59-69.

⁵⁸¹ SAID, Behnam T./FOUAD, Hazim (2018), opus cit., pp. 2-3.

República (GBA).⁵⁸² Es precisamente dentro de GTAZ en donde, en el año 2009, tuvo lugar la creación del primer grupo de trabajo sobre prevención, cuyos integrantes eran miembros de oficinas gubernamentales de inteligencia y de policía.⁵⁸³

Este grupo de trabajo sigue existiendo hoy en día y en la actualidad formula recomendaciones a fin de orientar sobre prácticas de prevención y desradicalización en Alemania. Sin embargo, si bien ya cuenta dentro de su equipo con expertos en comunicación, en la actualidad solo se limita a orientar y recomendar a los *Bundesländer* (estados federados), sin llegar a desarrollar ningún tipo de comunicación estratégica preventiva⁵⁸⁴ que sea de aplicación nacional.

A pesar de sus limitaciones, la labor de este grupo de trabajo ha sido siempre determinante dado que ha actuado como un foro de ideas y propuestas, y les ha permitido a los miembros de las agencias locales y federales intercambiar sus experiencias en esta materia.

Años después, se establecieron cambios en cuanto a quién o quiénes deberían de desempeñar dicha labor preventiva (especialistas, en lugar de miembros de servicios policiales), y desde donde, y se llegó a la conclusión de que:

«[...] los enfoques locales se adaptaban mejor a la estructura federal de Alemania y que un enfoque nacional era mucho menos deseable. Los enfoques locales se percibieron como más eficaces porque están más en sintonía con las circunstancias locales específicas y con las partes interesadas que pueden desempeñar un papel en la implementación de medidas concretas.»⁵⁸⁵

A partir de 2012, y durante los años siguientes a la toma de esta decisión, se crearon diversos centros de asesoramiento, tanto a nivel federal como a nivel estatal. No obstante, aunque aún eran pocos, se encontraban bien orientados y actuaban como modelo referencial para otros.

«Un ejemplo es la “Oficina de Asesoramiento sobre Radicalización” (*Beratungsstelle*) de la Oficina Federal para Migraciones y Refugiados (BAMF; una subunidad del BMI), que fue creada en 2012 y que ofrece una línea directa y un centro de asesoramiento para personas radicalizadas y sus familias.»⁵⁸⁶

En pocos años el crecimiento de esta forma preventiva fue tal que en 2018, la Oficina Federal de Investigación Criminal de Alemania (*Bundeskriminalamt*, BKA) “contabilizó 1.642

⁵⁸² Gemeinsames Terrorismusabwehrzentrum, GTAZ. (Centro Conjunto Contra el Terrorismo). Disponible en: https://www.bka.de/DE/UnsereAufgaben/Kooperation/GTAZ/gtaz_node.html [Fecha de consulta: 1 de diciembre de 2023].

⁵⁸³ Antes de este evento, en el año 1980 el Servicio Federal de Inteligencia (*Bundesnachrichtendienst*, BND) desarrolló un programa de reinserción social para terroristas de izquierda (RAF) por medio de un ‘plan de abandono’ del terrorismo, pero se desconoce si incluyó medidas P/CEV de aplicación específica. Véase: KOEHLER, Daniel (2021), opus cit., pp. 68-69.

⁵⁸⁴ De acuerdo con María Victoria Carrillo Durán, por comunicación estratégica se entiende “*el esfuerzo de gestión de la comunicación que hay que realizar a largo plazo [...] para conseguir que la relación con todos los públicos de interés vinculados a ella contribuya a sumar beneficios, en la línea de alcanzar los objetivos marcados en base a la misión y visión de la estrategia global. [...] La consecución de tales objetivos pondrá en marcha un mecanismo de acciones tácticas que se desdoblarán en planes de acción de comunicación, con una temporalidad definida, para el logro de los objetivos marcados a priori.*” Es decir, no nos referimos aquí a la necesidad de establecer un plan comunicativo de aplicación nacional, lo cual sería sin duda una equivocación, sino a establecer una comunicación que posea características comunes en todos los estados, que este orientada al cumplimiento de objetivos generales y específicos armonizados, y que se encuentre bajo la supervisión de una única oficina o unidad. Véase: CARRILLO DURÁN, María Victoria (2014): «La comunicación estratégica y sus profesionales», *Revista Mediterránea de Comunicación*, vol. 5, N.º 2, (22-46), p. 39.

⁵⁸⁵ “*Ejemplos de agentes de la sociedad civil que realizan el trabajo preventivo son la Red de Prevención de la Violencia (VPN) en Baviera y Hesse; VAJA y su proyecto “Kitab” en Bremen; Zentrum Demokratische Kultur y su iniciativa “Hayat” en Berlín; y Ambulante Maßnahmen Altona y la Fundación Pestalozzi con su proyecto común “Legato” en Hamburgo. Estas instituciones que desempeñan un papel vital en el enfoque de prevención de Alemania están dirigidas en su mayoría por trabajadores sociales o personas con experiencia de campo en el trabajo con jóvenes vulnerables.*” Véase: SAID, Behnam T./FOUAD, Hazim (2018), opus cit., p. 6.

⁵⁸⁶ *Ibidem*, p. 3.

programas y proyectos activos de P/CEV”⁵⁸⁷ Cabe señalar que el mayor incremento de programas de prevención contra el extremismo violento y desradicalización se dio entre los años 2015 y 2018, cuando, entre ambos años, tuvo lugar un salto cuantitativo de más del doble, dado que en el año 2015 se contabilizaban 721 programas preventivos.

El P/CEV alemán tuvo su nacimiento en el ámbito de inteligencia y policía gubernamental y su crecimiento inicial tuvo lugar sobre la base de la experiencia del trabajo social de campo. Durante todos esos años careció por completo de la asesoría de la academia universitaria y/o de expertos externos. Su desarrollo estuvo por tanto vinculado a ONG’s y a acciones concretas de programas gubernamentales. Esta característica ha hecho que hasta el día de hoy el modelo P/CEV de Alemania se haya desarrollado de forma híbrida, y que este conformado entre el sector público y la iniciativa privada,⁵⁸⁸ situación que impacta en la financiación del desarrollo de todos de sus programas.

Según Daniel Koehler, la financiación de los programas P/CEV en Alemania proviene del Estado, pero a través de dos vías. Por lado, se cuenta con la financiación del sector gubernamental que interviene de forma directa en los programas y es la que proviene de los *Bundesländer* (estados federados)⁵⁸⁹; y, por otro lado, se cuenta con la financiación que aportan las ONG’s, cuyas actividades a su vez han sido financiadas desde la sede gubernamental de Berlín.⁵⁹⁰

En enero de 2015, el Ministerio Federal de Familia, Tercera Edad, Mujeres y Juventud (*Bundesministerium für Familie, Senioren, Frauen und Jugend*, BMFSFJ) dio inicio al programa “Vive la Democracia” (“*Demokratie leben!*”)⁵⁹¹, “un amplio programa de financiación de iniciativas contra el extremismo de derecha e islamista con un presupuesto que, en 2017, ascendió a 104,5 millones de euros.”⁵⁹²

El soporte financiero a estos programas de prevención es tal que, según Koehler, la financiación se ha triplicado en este mismo periodo, pasando “de los 300.000 euros disponibles en 2015, [a una financiación que] aumentó 25 veces hasta alcanzar los 7,5 millones de euros en 2020.”⁵⁹³ Ello resulta indicativo de que existe una relación directa entre el aumento de financiación y la creación de más programas P/CEV, situación que parece ir en aumento conforme al autor.

En el año 2017, también el Ministerio Federal de Familia, Tercera Edad, Mujeres y Juventud (*Bundesministerium für Familie, Senioren, Frauen und Jugend*, BMFSFJ) anunció que se

⁵⁸⁷ KOEHLER, Daniel (2021), opus cit., p. 67.

⁵⁸⁸ *Ibidem*, p. 61.

⁵⁸⁹ “Una característica distintiva del panorama preventivo es el sistema federal de Alemania, que la distingue de otros países. Alemania tiene un gobierno federal, pero al mismo tiempo está dividida en 16 estados, cada uno de los cuales tiene sus propias estructuras gubernamentales, es decir, sus propios primeros ministros, así como sus propios ministerios del interior o de asuntos sociales. Estos estados cooperan con el gobierno federal y, a menudo, reciben fondos de programas federales. Si bien estos fondos generalmente se otorgan sujetos a ciertas condiciones, el gobierno federal no puede obligar a los estados a adoptar todas sus políticas. Esta es probablemente la razón principal por la que no existe una estrategia nacional formal que prescriba la implementación de políticas específicas de manera uniforme en todas las diferentes partes del país. Más bien, la idea es proporcionar un marco común de directrices, que los estados deberían observar cuando diseñan sus estrategias específicas.” Véase: SAID, Behnam T./FOUAD, Hazim (2018), opus cit., p. 2.

⁵⁹⁰ KOEHLER, Daniel (2021), opus cit., p. 61.

⁵⁹¹ “Live Democracy!” (“Vive la Democracia”). Bundesministerium für Familie, Senioren, Frauen und Jugend, BMFSFJ. Disponible en: <https://www.demokratie-leben.de/en/programme> [Fecha de consulta: 1 de diciembre de 2023].

⁵⁹² SAID, Behnam T./FOUAD, Hazim (2018), opus cit., pp. 3-4.

⁵⁹³ *Ibidem*.

otorgaría financiación a proyectos que se orienten a la detección temprana en escuelas para prevenir la radicalización dentro de estas instituciones educativas. Dichos programas estarían a cargo de los denominados ‘Servicios para Jóvenes Inmigrantes’ (*Jugendmigrationsdienste*).⁵⁹⁴ El objetivo de estos dos programas destinados a los jóvenes es que:

«[...] los trabajadores sociales ayuden a los jóvenes a desarrollar resiliencia contra las narrativas islamistas y ofrecer perspectivas vocacionales a quienes están en riesgo. La suposición subyacente es si estas narrativas sólo son atractivas para aquellos si pueden identificar sus problemas individuales con ellas. Si las vulnerabilidades subyacentes a la radicalización se resuelven de antemano, según la idea, menos personas se volverán extremistas.»⁵⁹⁵

El significativo monto de financiación y el permanente fomento para subvencionar proyectos es indicativo de que el Ministerio Federal de Familia, Tercera Edad, Mujeres y Juventud (*Bundesministerium für Familie, Senioren, Frauen und Jugend*, BMFSFJ) apoya los programas de prevención, aun cuando “son implementados por otros ministerios, que son responsables de las prisiones y las escuelas, respectivamente.”⁵⁹⁶

Con independencia de los proyectos desarrollados por los centros de asesoramiento (locales y regionales) también se han desarrollado proyectos de prevención de aplicación específica con las orientaciones más variadas. Por ejemplo, se han desarrollado programas específicos dirigidos a profesores “como ‘*Salam-Online*’ del Centro de Teología Islámica (ZIT) de la Universidad Wilhelms de Münster, que proporciona directrices para que los profesores contrarresten el discurso de odio en línea.”⁵⁹⁷ También se ha promovido un programa denominado ‘*Ufuq.de*’, con orientación pedagógica, que educa sobre aspectos como la inmigración o el islam y previene el extremismo,⁵⁹⁸ o proyectos dirigidos a jóvenes vulnerables, como *JAMIL*⁵⁹⁹ desarrollado en Bremen, orientado a desalentar la participación de los jóvenes en acciones de extremismo violento. En relación con el extremismo violento de extrema derecha se ha promovido la iniciativa de *EXIT-Deutschland*⁶⁰⁰ una organización que asesora personalmente y de forma online a personas que buscan abandonar movimientos o agrupaciones neonazis.

Sin embargo, aun con esta enorme cantidad de iniciativas, gubernamentales y no gubernamentales, resulta llamativo el hecho de que no exista ningún organismo centralizado que controle la estrategia comunicativa de P/CEV en Alemania. Cada proyecto, programa, centro de asesoramiento (locales y regionales) lleva adelante su propia comunicación sin atenerse a directrices nacionales. Podemos encontrar únicamente una tendencia porcentual respecto al tipo de extremismo violento que se previene. Según Koehler, “la principal ideología a la que están destinados los programas P/CEV es claramente de la extrema derecha: el 64% de

⁵⁹⁴ Los Servicios para Jóvenes Inmigrantes se encuentran adscriptos a la entidad educativa, pero se encuentran coordinados por diversas organizaciones no gubernamentales de la sociedad civil.

⁵⁹⁵ *Ibidem*, p. 5.

⁵⁹⁶ *Ibidem*.

⁵⁹⁷ Forschungswerkstatt Salam-Online, Zentrum für Islamische Theologie (ZIT), Universität Münster. Disponible en: <https://www.uni-muenster.de/ZIT/Religionspaedagogik/Projekte/salam-online.html> [Fecha de consulta: 1 de diciembre de 2023].

⁵⁹⁸ Pädagogik zwischen Islam, Islamfeindlichkeit und Islamismus. (Pedagogía, Educación Cívica y Prevención). Disponible en: <http://www.ufuq.de> [Fecha de consulta: 1 de diciembre de 2023].

⁵⁹⁹ JAMIL, Verein zur Förderung akzeptierender Jugendarbeit, Bremen. Disponible en: <https://vaja-bremen.de/teams/jamil/> [Fecha de consulta: 1 de diciembre de 2023].

⁶⁰⁰ EXIT-Deutschland. Disponible en: <https://www.buendnis-toleranz.de/archiv/themen/extremismus/161709/exit-deutschland> [Fecha de consulta: 1 de diciembre de 2023].

todas las iniciativas, mientras que las centradas en el extremismo islamista representan un 32%.”⁶⁰¹

Actualmente se intenta frenar la retórica de odio contra los musulmanes. A tenor de ello, el Ministerio Federal del Interior y de la Patria (*Bundesministerium des Innern und für Heimat*, BMI), ha publicado un informe, en agosto de 2023, en donde pone de manifiesto la necesidad de comenzar a trabajar sobre el creciente sentimiento anti-musulmán. En el prólogo de dicho documento, la Ministra Federal del Interior, Nancy Faeser, expresa que el informe presentado “proporciona por primera vez un inventario exhaustivo del fenómeno del sentimiento anti-musulmán en Alemania, sus efectos y manifestaciones.”⁶⁰² Este reciente informe dimensiona el fenómeno y pone de manifiesto la necesidad de nuevos programas para evitar extremismos violentos en dicho sentido. No obstante, como ya se ha dicho, al no contar con una estrategia comunicativa común no se puede anticipar si tal documento del Ministerio Federal del Interior será tomado en cuenta en programas de prevención.

A tenor de esta falta de certeza, Behnam Said y Hazim Fouad, expresan que “para generar confianza, los profesionales de PEV y CEV necesitan regulaciones estrictas y transparentes y una estrategia de comunicación pública armonizada a nivel nacional.”⁶⁰³ Quizás entonces, después de este paso a nivel nacional, podríamos comenzar a hablar de una casi perfecta armonización a nivel europeo en esta materia.

A continuación, se incluirá una gráfica que enunciará las medidas adoptadas dentro de la Política Criminal alemana respecto al delito de terrorismo. Conforme se vayan analizando las medidas análogas de los otros Estados (Reino Unido y España), se irá completando la información faltante, de tal forma que al finalizar el análisis del último país estaremos en posición de presentar un cuadro comparativo que sintetizará la orientación que posee cada una de las medidas adoptadas dentro de la Política Criminal de cada Estado en cuestión.

Podemos concluir parcialmente que Alemania utiliza el Derecho penal del ciudadano, conforme no ha querido crear una legislación especial para el delito de terrorismo, y tiende a ser muy crítica en la utilización de las excepciones penales. Por otra parte, tiende a someter sus leyes penales a controles de constitucionalidad, a fin de determinar que no se alejan de los derechos fundamentales. El sistema institucional de Alemania otorga gran apoyo a las medidas preventivas de P/CEV, aunque naturalmente cuenta con medidas que ingresan dentro la seguritización del Estado, como unidades de inteligencia, agentes encubiertos, cibervigilancia, etc., tiende a focalizar su interés en el desarrollo de medidas dentro de su Política Criminal que no se caractericen por ser coercitivas. El modelo preventivo naturalmente es mixto porque cuenta con medidas punitivas (Derecho penal), medidas correctivas (P/CEV) y medidas mecánicas (cibervigilancia). Todo ello hace que la Política Criminal alemana pueda ser considerada dentro de *Lawfare*, es decir se desarrolla una lucha contra el terrorismo, pero siempre dentro de instancias judiciales y en el respeto de derechos constitucionales nacionales e internacionales.

⁶⁰¹ KOEHLER, Daniel (2021), opus cit., p. 67.

⁶⁰² FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY. FEDERAL GOVERNMENT (2023): *Report of the Independent Expert Group on Anti-Muslim Sentiment*, August 2023, Berlin, (1-370), p. 1.

⁶⁰³ SAID, Behnam T./ FOUAD, Hazim (2018), opus cit., p. 11.

Tabla 4: Medidas de la Política Criminal de Alemania respecto al delito de terrorismo.

TERRORISMO	ALEMANIA	REINO UNIDO	ESPAÑA
Derecho Penal	Derecho penal del ciudadano		
Sistema Institucional	P/CEV		
Modelo Preventivo	Mixto (punitivo, correctivo, mecánico)		
Tendencia de la Política Criminal	Lawfare		

Fuente: Elaboración propia. 2023.

CAPÍTULO 9: REINO UNIDO

LA POLÍTICA CRIMINAL DE REINO UNIDO EN MATERIA DE TERRORISMO

Dentro de su Política Criminal, para Reino Unido es vital utilizar todos los medios a su disposición para desviar a la gente de las actividades relacionadas con el terrorismo, y para evitar la comisión de atentados terroristas.

A lo largo de los años, Reino Unido ha fortalecido sus capacidades antiterroristas en todo su territorio. Entre 1969 y 2000, Reino Unido y principalmente sus cuerpos policiales desarrollaron una gran competencia en la lucha antiterrorista, principalmente debido a la existencia de terrorismo de origen irlandés durante el periodo señalado. Sí bien, hoy en día sigue existiendo un control sobre dicha actividad terrorista, toda la lucha antiterrorista se ha centrado en el terrorismo yihadista, sobre todo luego del 11S, y es precisamente sobre esta lucha que se ha configurado su actual Política Criminal en la materia.

En el presente, Reino Unido continúa buscando formas de mejorar dicha capacidades. La utilización de un enfoque colectivo aunado bajo una misma estrategia nacional (Estrategia CONTEST⁶⁰⁴) es el paraguas bajo el cual trabajan en materia antiterrorista el sector público (gobierno, ministerios, sistema educativo, sanidad, policía nacional, local y antiterrorista, unidades de inteligencia, sistema legal y penitenciario, urbanismo, etc.), y el sector privado (universidades o centros educativos privados, empresas de tecnología, empresas de entretenimiento masivo, *think tanks*, medios de comunicación, organizaciones no gubernamentales, asociaciones profesionales, centros deportivos y clubes de fútbol, centros comunitarios, etc.), que actúa como socio del primero.

Consciente de que las fronteras nacionales no limitan las actividades del terrorismo, Reino Unido también se encuentra comprometido a trabajar con socios internacionales, para abordar junto a los Estados Miembros de la Unión Europea y a terceros Estados, coyunturas que las organizaciones terroristas pueden aprovechar para ampliar su apoyo global, como conflictos regionales, territorios con oportunidades educativas o laborales limitadas, o la ausencia de vías legítimas para expresar diversas opiniones o la restringida participación en la sociedad que tiene la ciudadanía de algunos países. En este segmento trabaja en colaboración con sus socios internacionales para mejorar las condiciones de los territorios que podrían ser cuna de la actividad terrorista en Europa.

Adicionalmente, Reino Unido desarrolla todo un trabajo en materia antiterrorista en Internet. Su intervención, principalmente preventiva en este ámbito, representa una labor inmensa que agrupa centros especializados, unidades de análisis, referencias de contenido terrorista, desarrollo de campañas preventivas en diversos formatos, etc. Dicho trabajo en el ciberespacio, como se explicará en las siguientes páginas, ha servido de inspiración para la creación de la Unidad de Referencia de Internet de la Unión Europea (EU IRU).

⁶⁰⁴ CONTEST es la amplia estrategia de Reino Unido contra el terrorismo cuyos objetivos se basan en las cuatro “P”: Perseguir, Prevenir, Proteger y Preparar.

Todas las actividades desarrolladas en Reino Unido en materia antiterrorista se encuentran contenidas dentro de las leyes vigentes. Reino Unido posee un derecho especial para los delitos de terrorismo que le permite ciertas excepciones y que sitúan la legislación británica en lo que conocemos como Derecho penal del enemigo.

En este sentido se cuenta con un paquete de medidas legales para reducir las acciones de quienes participan en actividades relacionadas con el terrorismo. La legislación británica prevé diversos delitos de terrorismo en las Leyes de Terrorismo y Antiterrorismo de 2000, 2006, 2008 y 2015. Además, la Ley de Medidas de Prevención e Investigación del Terrorismo de 2011 proporciona al Ministro del Interior (*Home Office*) un mecanismo para otorgar un tratamiento jurídico como ‘sospechoso de terrorismo’ a quien, por diversos motivos procesales, aún no se puede procesar o deportar.

A su vez, el gobierno también puede congelar y, cuando corresponda, decomisar los activos de los terroristas conforme a la Ley de Congelación de Activos Terroristas, etc. de 2010, y la Ley contra el Terrorismo, la Delincuencia y la Seguridad de 2001.

Además de los delitos tipificados en estas leyes, la policía (nacional, local y antiterrorista) y la Fiscalía de la Corona poseen potestad para investigar y poner a disposición judicial a los terroristas, cuando corresponda, por cualquier otro delito penal, a fin de interrumpir o perturbar de forma efectiva su actividad.⁶⁰⁵

En adición al modelo institucional y legislativo, la retórica gubernamental está focalizada en considerar a los terroristas como enemigos, mientras que, a su vez, el tratamiento informativo de las noticias relacionadas con el terrorismo en Reino Unido se orienta a un posicionamiento de guerra dentro del Estado.

LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL BRITANICA

INSTRUMENTOS NORMATIVOS PARA LA PERSECUCIÓN DEL TERRORISMO ONLINE

El elemento central de la legislación antiterrorista del Reino Unido es su Ley contra el Terrorismo de 2000 (*Terrorism Act 2000*).⁶⁰⁶ Este instrumento se estableció para proporcionar una legislación permanente en todo el Reino Unido a fin de cubrir todas las formas de terrorismo. La definición de terrorismo recogida en la Ley contra el Terrorismo de 2000 es:

⁶⁰⁵ Por ejemplo, el Anexo 7 de la Ley contra el Terrorismo de 2000 (*Terrorism Act 2000*) permite a agentes de policía detener e interrogar (y cuando sea necesario, detallar y registrar), sin sospecha, a cualquier individuo que atravesase un puerto de entrada o la zona fronteriza, para determinar si esa persona parece ser alguien que está o ha estado involucrado en la comisión, preparación o instigación de actos de terrorismo. Véase: Anexo 7, Sección Proteger.

⁶⁰⁶ *Terrorism Act 2000*. Disponible en: <https://www.legislation.gov.uk/ukpga/2000/11/contents> [Fecha de consulta: 11 diciembre de 2023].

«El uso o amenaza de una acción específica cuando el uso o amenaza está diseñado para influir en el gobierno o intimidar al público o a una sección del público, y el uso o amenaza se hace con el propósito de promover una causa política, religiosa o ideológica. La acción es una acción específica si involucra violencia grave contra una persona; implica daños graves a la propiedad; pone en peligro la vida de una persona, distinta de la de la persona que comete la acción; crea un riesgo grave para la salud o la seguridad del público o de una sección del público; o está diseñada para interferir seriamente o alterar gravemente un sistema electrónico.»⁶⁰⁷

La Ley contra el Terrorismo de 2000 prevé los siguientes delitos:

- «Divulgación a otra persona de información que podría perjudicar una investigación terrorista, o interferir con material relevante para dicha investigación.»⁶⁰⁸
- «Proporcionar o recibir instrucción o capacitación en la fabricación o uso de armas de fuego, explosivos, material radiactivo o armas diseñadas o adaptadas para la descarga de cualquier material radiactivo, armas químicas, biológicas o nucleares; o invitar a otra persona a recibir dicha formación, dentro o fuera de Reino Unido.»⁶⁰⁹
- «Dirigir las actividades de una organización involucrada en la comisión de actos de terrorismo.»⁶¹⁰
- «Posesión de un artículo con fines relacionados con la comisión, preparación o instigación de actos de terrorismo.»⁶¹¹
- «Recopilar o registrar información de un tipo que pueda ser útil para una persona que cometa o prepare un acto de terrorismo o poseer un documento o registro que contenga dicha información, o acceder a documentos o consultar dicha información a través de Internet.»⁶¹²
- «Incitación de otra persona a cometer un acto de terrorismo total o parcialmente fuera de Reino Unido, cuando ese acto constituiría un delito de asesinato, herir intencionalmente, envenenamiento, delitos con explosivos y poner en peligro la vida mediante daños a la propiedad.»⁶¹³

⁶⁰⁷ Sección 1 de la Ley contra el Terrorismo de 2000. Cuando el uso o la amenaza de acción involucre armas de fuego o explosivos, será terrorismo, ya sea que esté diseñado o no para influir en un gobierno o para intimidar al público.

⁶⁰⁸ Sección 39 (2) (a) y (b) de la Ley contra el Terrorismo de 2000. Según la Sección 39 (7) (a) la comisión de alguno de estos delitos conlleva una pena máxima de cinco años de prisión.

⁶⁰⁹ Sección 54 (1) (a), (aa), (b) y (c) de la Ley contra el Terrorismo de 2000. Según la Sección 54 (6) la comisión de alguno de estos delitos en su forma más grave conlleva la pena de cadena perpetua. La pena de cadena perpetua se introdujo mediante la enmienda recogida el 13/4/2015 en *Criminal Justice and Courts Act 2015* (Ley de Tribunales y Justicia Penal 2015), Sección 1 (2). Antes de dicha enmienda la pena máxima era de diez años de prisión.

⁶¹⁰ Sección 56 (1) de la Ley contra el Terrorismo de 2000. Según la Sección 56 (2) la comisión de alguno de estos delitos conlleva una pena máxima de cadena perpetua.

⁶¹¹ Sección 57 (1) de la Ley contra el Terrorismo de 2000. Según la Sección 57 (4) (a) la comisión de alguno de estos delitos conlleva una pena máxima de quince años de prisión. Antes de la enmienda de 2006, recogida el 13/4/2006 en *Terrorism Act 2006* (Ley contra el Terrorismo de 2006), Sección 13 (1), la pena máxima era de diez años de prisión.

⁶¹² Sección 58 (1) (a), (b) y (c) de la Ley contra el Terrorismo de 2000. Según la Sección 58 (3A) (4) la comisión de alguno de estos delitos conlleva una pena máxima de quince años de prisión. Antes de la enmienda de 2019, recogida el 12/4/2019 en *Counter-Terrorism and Border Security Act 2019* (Ley de Seguridad Fronteriza y Antiterrorismo de 2019), Sección 7 (3), la pena máxima era de diez años. Cabe señalar que la Sección 58 (3A) (b) excluye de esta acusación a periodistas y académicos acreditados en el ejercicio de su trabajo. Sin embargo, sí sería susceptible de acusación ciudadanos que revisaran voluntariamente y con conocimiento dicho material aún sin la intención probada de cometer posteriormente un atentado, a excepción de aquellos que pudieran demostrar que desconocían la existencia de contenido terrorista en las publicaciones o documentos consultados según la Sección 58 (3A) (a). En estos casos se prevé multa o pena de prisión de 6 meses de acuerdo con la Sección 58 (4) (b).

⁶¹³ Sección 59 (1) (a) y 59 (2) (a), (b), (c), (d) y (e) de la Ley contra el Terrorismo de 2000. Una persona culpable de un delito previsto en esta sección estará sujeta a cualquier pena que se le imponga si es condenada por el delito enumerado en el inciso (2) que corresponda al acto que incita.

- «No revelar información que pueda prevenir un acto de terrorismo o asegurar la detención, el procesamiento o la condena de otra persona por un delito que implique la comisión, preparación o instigación de un acto de terrorismo.»⁶¹⁴

Además de desarrollar un amplio marco de tipificaciones, la Ley contra el Terrorismo de 2000 también mejora los poderes de la policía para contrarrestar e investigar el terrorismo, e incluye disposiciones para detener y registrar a peatones y vehículos⁶¹⁵, así también como para restringir el estacionamiento.⁶¹⁶ No obstante, siempre que los poderes para detener y registrar deban de ejercerse por un plazo de tiempo mayor a 48 horas, deben de ser autorizados por un oficial superior designado y confirmado por el Secretario de Estado.

Los funcionarios de policía, aduanas e inmigración también adquieren poderes antiterroristas ampliados para detener, interrogar, detener y registrar a personas en los puertos (incluidos aeropuertos) y exigirles que presenten una identificación.

En el marco de esta Ley se facultó también al Secretario de Estado para ejercer la prohibición de grupos que son valorados como una preocupación con relación al terrorismo. En consecuencia, hasta la fecha, en todo Reino Unido unas 80 organizaciones terroristas internacionales⁶¹⁷ han sido prohibidas en virtud de la Ley contra el terrorismo de 2000.⁶¹⁸

La proscripción o prohibición de una organización terrorista acarrea, por asociación, la tipificación de tres delitos graves. Estos son, ser miembro o profesar pertenecer a una organización proscrita⁶¹⁹, apoyar a una organización proscrita⁶²⁰, usar una prenda de vestir o usar, llevar o exhibir un artículo en público que despierte una sospecha razonable de que una

⁶¹⁴ Sección 38B (1) (a) y (b) de la Ley contra el Terrorismo de 2000. Según la Sección 38B (5) (a) la comisión de alguno de estos delitos conlleva una pena máxima de diez años de prisión. Antes de la enmienda de 2019, recogida el 12/4/2019 en *Counter-Terrorism and Border Security Act 2019* (Ley de Seguridad Fronteriza y Antiterrorismo de 2019), Sección 7 (2) la pena máxima era de cinco años.

⁶¹⁵ Sección 44 (1) y (2) de la Ley contra el Terrorismo de 2000.

⁶¹⁶ Sección 48 de la Ley contra el Terrorismo de 2000.

⁶¹⁷ En total, a la fecha, existen 94 organizaciones prohibidas en Reino Unido, debido a que 14 organizaciones calificadas como terroristas ya estaban proscritas según la legislación anterior en Irlanda del Norte.

⁶¹⁸ El acto formal de prohibición está a cargo del Parlamento Británico, y la petición se hace mediante la entrega de un dossier que incluye todo tipo de información, como los objetivos de los grupos, que justifica el pedido de proscripción al Parlamento. El último grupo terrorista en ser prohibido, en enero de 2024, ha sido *Hizb ut-Tahrir* [prohibida desde el 15 de enero de 2003 en Alemania] una “organización política islamista sunita internacional fundada en Jerusalén en 1953 por el jeque Taquiddin an-Nabhani. Hizb ut-Tahrir tiene presencia en al menos 32 países, con su sede y su Oficina Central de Medios (CMO) con sede en Beirut, Líbano. La CMO gestiona el sitio web central de propaganda de Hizb ut-Tahrir, hizb-ut-tahrir.info. El objetivo declarado a largo plazo de Hizb ut-Tahrir es unificar a los musulmanes en todo el mundo y establecer un califato regido bajo la ley islámica (Sharia). Hizb ut-Tahrir Britain es la rama oficial de Hizb ut-Tahrir en el Reino Unido y se estableció en el Reino Unido en la década de 1980. El gobierno del Reino Unido evalúa que Hizb ut-Tahrir Gran Bretaña es una rama componente de Hizb ut-Tahrir, pero se le otorga autonomía para interpretar y abordar la estrategia global de Hizb ut-Tahrir de acuerdo con su entorno local. El gobierno del Reino Unido evalúa que Hizb ut-Tahrir, incluidas sus ramas nacionales, está actualmente involucrado en terrorismo y cumple con el criterio de ‘promueve y alienta’ de la prueba legal. Se publicaron varios artículos en línea en el sitio web central de medios de Hizb ut-Tahrir (y en sitios web de terceros), atribuidos a varias de las ramas de Hizb ut-Tahrir, que celebraron y elogiaron el ataque del 7 de octubre de 2023 por parte de Hamás y los eventos asociados. El contenido de estos artículos, muchos de los cuales se refieren a Hamás como ‘héroes’ y alientan nuevas actividades terroristas, constituyen la promoción y el estímulo del terrorismo.” Véase: «Proscribed terrorist groups or organisations», Home Office. Disponible en: <https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations-2/proscribed-terrorist-groups-or-organisations-accessible-version#list-of-proscribed-international-terrorist-groups> [Fecha de consulta: 19 de enero de 2024].

⁶¹⁹ Sección 11 (1) de la Ley contra el Terrorismo de 2000. Según la Sección 11 (3) (a) la comisión de alguno de estos delitos conlleva una pena máxima de catorce años de prisión. Antes de la enmienda de 2021, recogida el 29/6/2021 en *Counter-Terrorism and Sentencing Act 2021* (Ley de Sentencias y Antiterrorismo de 2021), Sección 26 (1) (a), la pena máxima era de 10 años prisión.

⁶²⁰ Sección 12 (1) (a) de la Ley contra el Terrorismo de 2000. Según la Sección 12 (6) (a) la comisión de alguno de estos delitos conlleva una pena máxima de catorce años de prisión. Antes de la enmienda de 2021, recogida el 29/6/2021 en *Counter-Terrorism and Sentencing Act 2021* (Ley de Sentencias y Antiterrorismo de 2021), Sección 26 (1) (b), la pena máxima era de 10 años prisión.

persona apoya o es miembro de una organización proscrita.⁶²¹ La Ley también establece que las acciones en beneficio de una organización⁶²² que ha sido clasificada como prohibida en Reino Unido, son acciones que se consideran con fines terroristas.

En cuanto a la financiación del terrorismo, la Ley contra el Terrorismo del año 2000 tipifica cuatro delitos principales. Estos son, recaudación de fondos (se considera un delito invitar a cualquier persona a proporcionar dinero o bienes, a recibir dinero o bienes, o en primera persona proporcionar dinero o bienes. Todo ello con fines terroristas)⁶²³, uso y posesión de dinero o bienes con fines terroristas⁶²⁴, participación en acuerdos financieros mediante los cuales sumas de dinero o bienes se ponen a disposición de finalidad terroristas⁶²⁵, y lavado de dinero.⁶²⁶ Adicionalmente existe la obligación, en virtud de esta Ley, de revelar cualquier conocimiento o sospecha de financiación del terrorismo basándose en información que surja del ejercicio regular del propio oficio, profesión, negocio o empleo.⁶²⁷ No revelar dicha información constituye un delito.

La Ley contra el Terrorismo de 2000 encuentra refuerzos en la lucha contra el delito de financiación del terrorismo, debido a que Reino Unido establece nuevas disposiciones jurídicas en la Ley contra el Terrorismo, la Delincuencia y la Seguridad (ATCS) de 2001.⁶²⁸ Por medio de la Ley ATCS, los funcionarios autorizados (agentes, funcionarios de aduanas o funcionarios de inmigración) pueden confiscar y detener efectivo si tienen motivos razonables para sospechar que se trata de efectivo que brinde soporte o algún tipo de apoyo a las actividades terroristas.⁶²⁹ El dinero incautado debe ser liberado en un plazo de 48 horas, a menos que un tribunal de primera instancia emita una orden que permita una mayor detención por hasta tres meses.⁶³⁰ Las órdenes de detención pueden dictarse si existen motivos y justificación razonables para hacerlo, y pueden renovarse, para retener el dinero el curso de una investigación por un período máximo de dos años.

La Ley ATCS surge en respuesta a los ataques terroristas del 11 de septiembre de 2001, y se basa en disposiciones antiterroristas que ya están vigentes en el Reino Unido con el objeto de garantizar que el Gobierno tenga los poderes esenciales para contrarrestar todas las formas de amenaza terrorista. Ello significa que este instrumento jurídico no ha creado nuevas tipificaciones, (a excepción de una en concreto que se mencionará a continuación), sino que, a partir del hecho histórico señalado, se reforzaron en Reino Unido los poderes antiterroristas que ya estaban siendo utilizados en muchas áreas.

⁶²¹ Sección 13 (1) (a) y (b) de la Ley contra el Terrorismo de 2000. Según la Sección 13 (3) (a) la comisión de alguno de estos delitos conlleva una pena máxima de seis meses de prisión.

⁶²² Por ejemplo, financiar o ayudar al financiamiento de dicha organización.

⁶²³ Sección 15 (1) (a) (b), 2 (a) (b) y 3 (a) (b) de la Ley contra el Terrorismo de 2000.

⁶²⁴ Sección 16 (2) (a) y (b) de la Ley contra el Terrorismo de 2000.

⁶²⁵ Sección 17 (a) y (b) de la Ley contra el Terrorismo de 2000.

⁶²⁶ Sección 18 (1) (a) (b) (c) y (d) de la Ley contra el Terrorismo de 2000.

⁶²⁷ Sección 19 (1) (a) y (b) de la Ley contra el Terrorismo de 2000.

⁶²⁸ *Anti-Terrorism, Crime and Security Act 2001* (ATCS Act 2001). Disponible en: <https://www.legislation.gov.uk/ukpga/2001/24/contents> [Fecha de consulta: 29 de diciembre de 2023].

⁶²⁹ Anexo 1, párrafos 2 y 3 de la Ley ATCS.

⁶³⁰ Anexo 1, párrafo 3 de la Ley ATCS.

Las medidas clave de la Ley ATCS de 2001 se basan en establecer disposiciones adicionales sobre armas de destrucción masiva⁶³¹, también en establecer disposiciones adicionales que exigen la divulgación de sospechas de actividades de financiación del terrorismo⁶³², en mejorar la seguridad de patógenos y toxinas, (incluidos poderes para inspeccionar las instalaciones y negar el acceso a las instalaciones a personas determinadas)⁶³³, en brindar poderes adicionales a funcionarios para proceder al arresto y expulsión de personas dentro de aeronaves y de aeropuertos⁶³⁴, para regular la seguridad de la aviación en general⁶³⁵, para detener aeronaves⁶³⁶, así también como para acrecentar la intervención de comunicaciones aeronáuticas y datos de tráfico.⁶³⁷ La Ley ATCS de 2001 también ha permitido la creación de un delito de uso de sustancias nocivas y sustancias para dañar o intimidar⁶³⁸, y finalmente, otorgar al Estado mayores poderes de congelación de activos cuando un individuo, entidad o país representa un riesgo para la economía del Reino Unido, la vida o la propiedad de los nacionales o residentes del Reino Unido.⁶³⁹

A estas medidas adoptadas mediante la Ley ATCS se le suman las medidas de la Orden contra el Terrorismo de 2006.⁶⁴⁰ La Orden SI 2006/2657, prohíbe cualquier trato con fondos y recursos económicos de personas designadas por el Tesoro como sospechosas de estar involucradas en terrorismo y prohíbe a las personas poner fondos, recursos económicos y servicios financieros a disposición de dichas personas a menos que tengan autorización del Tesorería. La Orden tipifica como delito el incumplimiento de estas prohibiciones. El Banco de Inglaterra, en calidad de agente del Tesoro, mantiene una lista de personas designadas.

En este mismo asunto, existen medidas análogas en el marco de la Unión Europea en virtud del Reglamento (CE) 2580/2001 del Consejo, que implementa la Posición Común de la Unión respecto a este delito. Por tanto, la Orden SI 2006/2657 constituye una herramienta jurídica dentro del Derecho penal de Reino Unido que se construye de forma híbrida dado que asegura la aplicación de las recomendaciones de las Naciones Unidas y a su vez la aplicación del Reglamento del Consejo de la Unión Europea.

En el año 2006 tiene lugar la adopción de la Ley contra el Terrorismo de 2006 (*Terrorism Act 2006*).⁶⁴¹ Esta Ley se crea en Reino Unido como respuesta interna a los ataques terroristas del 7 de julio de 2005 perpetrados en Londres. La nueva Ley contra el Terrorismo de 2006 establece disposiciones más amplias e introduce una serie de delitos nuevos que están relacionados con

⁶³¹ Secciones 43 a 57 de la Ley ATCS.

⁶³² Anexo 2, Parte 3, de la Ley ATCS.

⁶³³ Secciones 58 a 75 de la Ley ATCS.

⁶³⁴ Secciones 82 a 84 de la Ley ATCS.

⁶³⁵ Sección 85 de la Ley ATCS.

⁶³⁶ Sección 86 de la Ley ATCS.

⁶³⁷ Secciones 102 a 107 de la Ley ATCS.

⁶³⁸ Sección 113 de la Ley ATCS. Esta sección fue modificada en mediante la Ley contra el Terrorismo de 2006 (*Terrorism Act 2006*), al incluir también, juntamente con los gobiernos y el sector público, a las Organizaciones Internacionales como destinatarias de los ataques terroristas.

⁶³⁹ Sección 114 de la Ley ATCS.

⁶⁴⁰ La Orden contra el Terrorismo de 2006 (SI 2006/2657), busca adoptar respecto a la financiación del terrorismo y congelación de activos, los requisitos expresados en la Resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas. Véase: *The Terrorism (United Nations Measures) Order 2006* (SI 2006/2657). Disponible en: <https://www.legislation.gov.uk/ukxi/2006/2657/contents/made> [Fecha de consulta: 28 de diciembre de 2023].

⁶⁴¹ *Terrorism Act 2006*. Disponible en: <https://www.legislation.gov.uk/ukpga/2006/11/contents> [Fecha de consulta: 29 de diciembre de 2023]. La Ley contra el Terrorismo de 2006 (*Terrorism Act 2006*)

los usos de Internet por parte del terrorismo y/o con fines terroristas. Estas nuevas tipificaciones a la vez refuerzan la armonización penal dentro de la Unión Europea con relación a esta materia.

De esta forma, en la Ley contra el Terrorismo de 2006 podemos encontrar las siguientes nuevos delitos:

1. *Encouragement of terrorism* (Fomento al terrorismo)⁶⁴²

Dentro de la Sección 1 de la Ley contra el Terrorismo de 2006, se tipifica como delito la publicación o incitar a que se publique una declaración que, directa o indirectamente, aliente a otros a cometer actos de terrorismo. Esto incluye declaraciones que glorifiquen la comisión o preparación de actos de terrorismo. Ser acusado de este delito conlleva una pena máxima de quince años de prisión. Cabe señalar que la Ley de Seguridad Fronteriza y Antiterrorismo de 2019 (*Counter-Terrorism and Border Security Act 2019*)⁶⁴³ incrementó la pena de prisión de esta tipificación conforme antes de la modificación de 2019, la pena de prisión era de siete años.⁶⁴⁴

2. *Dissemination of terrorist publications* (Difusión de publicaciones terroristas)⁶⁴⁵

En la Sección 2 de la Ley contra el Terrorismo de 2006 se tipifica la venta, préstamo u otra difusión de publicaciones terroristas. Se define también dentro de esta tipificación que se entiende por publicación terrorista, reconociendo que es aquella que contiene material que fomenta el terrorismo, o bien que resulta de utilidad para los terroristas. Ser acusado de este delito conlleva una pena máxima de quince años de prisión. Al igual que con el delito de fomento al terrorismo, cabe señalar que la pena de prisión también era de siete años antes de la modificación que introdujo la Ley de lucha contra el Terrorismo y Seguridad Fronteriza de 2019.⁶⁴⁶

3. *Preparation of terrorist acts* (Actos preparatorios de acciones terroristas)⁶⁴⁷

Dentro de la Sección 5 de la Ley contra el Terrorismo de 2006, se penalizan los actos preparatorios de acciones terroristas. El objetivo de esta tipificación es detener y enjuiciar a quienes tienen la intención de cometer o ayudar a otros a cometer actos de terrorismo y que para ello deben de tomar medidas para prepararse y para hacer efectiva dicha intención. Ser acusado de este delito conlleva la pena cadena perpetua.

⁶⁴² Sección 1 de la Ley contra el Terrorismo de 2006.

⁶⁴³ *Counter-Terrorism and Border Security Act 2019*. Disponible en: <https://www.legislation.gov.uk/ukpga/2019/3/contents> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁴⁴ “In section 1 (encouragement of terrorism), in subsection (7)(a), for ‘7 years’ substitute ‘15 years’”. Véase: *Terrorism and Border Security Act 2019*. (12/04/2019).

⁶⁴⁵ Sección 2 de la Ley contra el Terrorismo de 2006.

⁶⁴⁶ “In section 2 (dissemination of terrorist publications), in subsection (11)(a), for ‘7 years’ substitute ‘15 years’”. Véase: *Terrorism and Border Security Act 2019*. (12/04/2019).

⁶⁴⁷ Sección 5 de la Ley contra el Terrorismo de 2006.

4. *Preparation of terrorist acts and terrorist training* (Preparación de actos terroristas y entrenamiento terrorista.)⁶⁴⁸

La Sección 6 denominada *Training for terrorism* (Entrenamiento para el terrorismo) de la Ley contra el Terrorismo de 2006 garantiza que cualquiera que brinde o reciba instrucción o capacitación a fin de aprender o consolidar técnicas o habilidades para cometer actos terroristas pueda ser procesado. Esto incluye (a) la fabricación, manipulación o uso de una sustancia nociva, o de sustancias de una descripción de dichas sustancias, y (b) el uso de cualquier método o técnica para hacer cualquier otra cosa que pueda hacerse con fines terroristas, en relación con la comisión o preparación de un acto de terrorismo. Ser acusado de este delito conlleva la pena de cadena perpetua.

Por otra parte, la tipificación denominada *Attendance at a place used for terrorist training* (Asistencia a un lugar utilizado para entrenamiento terrorista) recogida en la Sección 8 de la Ley contra el Terrorismo de 2006 establece como delito la asistencia a un lugar de entrenamiento terrorista en donde se imparta instrucción o capacitación, total o parcialmente, con fines relacionados con la comisión o preparación de actos de terrorismo. Ser acusado de este delito conlleva una pena máxima de catorce años de prisión. Cabe señalar que la Ley de Sentencias y Antiterrorismo de 2021 (*Counter-Terrorism and Sentencing Act 2021*)⁶⁴⁹ incrementó la pena de prisión de esta tipificación conforme antes de la modificación de 2021, la pena de prisión era de diez años.⁶⁵⁰

5. *Offences involving radioactive devices and materials and nuclear facilities and sites* (Delitos relacionados con dispositivos y materiales radiactivos e instalaciones y emplazamientos nucleares)⁶⁵¹

Conforme a la Sección 9, denominada *Making and possession of devices or materials* (Fabricación y posesión de dispositivos o materiales) de la Ley contra el Terrorismo de 2006, constituye delito fabricar o poseer un dispositivo radiactivo o poseer material radiactivo con la intención de utilizarlo con fines terroristas. (4) En esta sección ‘Dispositivo radiactivo significa (a) arma nuclear u otro dispositivo explosivo nuclear, (b) un dispositivo de dispersión de material radiactivo, o (c) un dispositivo emisor de radiación. En cualquier caso, ser acusado de este delito conlleva la pena cadena perpetua. De acuerdo con a la Sección 10 *Misuse of devices or material and misuse and damage of facilities* (Mal uso de dispositivos o material y mal uso y daño de las instalaciones) de la Ley contra el Terrorismo de 2006 constituye un delito hacer un uso indebido de un dispositivo o material radiactivo o dañar una instalación nuclear con fines terroristas. Una persona comete este delito si, en el curso o en relación de un acto de terrorismo o con fines terroristas, utiliza o daña una instalación nuclear de una manera que (a) provoque liberación de material radiactivo, o (b) crea o aumenta un riesgo de que dicho material sea liberado. Ser acusado de este delito conlleva la pena de cadena perpetua.

⁶⁴⁸ Secciones 6 y 8 de la Ley contra el Terrorismo de 2006.

⁶⁴⁹ *Counter-Terrorism and Sentencing Act 2021*. Disponible en: <https://www.legislation.gov.uk/ukpga/2021/11/contents> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁰ “In the Terrorism Act 2006, in section 8(4)(a) (sentence on conviction on indictment for attendance at place used for terrorist training), for ‘10’ substitute ‘14’”. Véase: *Counter-Terrorism and Sentencing Act 2021*.

⁶⁵¹ Secciones 9 a 11 de la Ley contra el Terrorismo de 2006.

Según la Sección 11 denominada *Terrorist threats relating to devices, materials or facilities* (Amenazas terroristas relacionadas con dispositivos, materiales o instalaciones) de la Ley contra el Terrorismo de 2006, constituye un delito hacer exigencias en el curso de un acto de terrorismo o con fines de terrorismo en relación con el suministro o el acceso a un dispositivo radiactivo, material radiactivo o una instalación nuclear, o si la exigencia hace suponer que existe un riesgo real de que la amenaza se lleve a cabo si no se cumple la exigencia. También es delito amenazar con utilizar material radiactivo, un dispositivo radiactivo o dañar una instalación nuclear en el curso de un acto de terrorismo o con fines terroristas. Ser acusado de este delito conlleva la pena de cadena perpetua.

En términos generales, la legislación antiterrorista de Reino Unido ha evolucionado para mantener y reforzar la capacidad del Estado de luchar contra las amenazas terroristas que se encuentran en constante cambio. La Ley de Seguridad Fronteriza y Antiterrorismo de 2019 (*Counter-Terrorism and Border Security Act 2019*), y la Ley de Sentencias y Antiterrorismo de 2021 (*Counter-Terrorism and Sentencing Act 2021*) son dos leyes que refuerzan las leyes previas (Ley de 2000 y Ley de 2006) en cuanto a la punición de los delitos, focalizando el fortalecimiento de la normativa mayormente en el incremento de las penas privativas de prisión. En ambas leyes, respecto de la Ley contra el Terrorismo de 2000 y la Ley contra el Terrorismo de 2006, tienen lugar incrementos de las penas privativas de libertad, y/o se generan matizaciones conceptuales en la redacción de las disposiciones. La Ley de Seguridad Fronteriza y Antiterrorismo de 2019 procuró la eliminación de lagunas en la legislación a fin de garantizar que la legislación no se aplique con discrecionalidad y para que sea funcional a la era digital al considerar los patrones actuales de reclutamiento y radicalización mediante Internet. Por su parte, cabe destacar que la Ley de Sentencias y Antiterrorismo de 2021 ha implementado la mayor reforma legislativa de las últimas décadas, concretamente en cuanto a las condenas y al seguimiento de los terroristas de forma posterior al cumplimiento de la pena. Las medidas incluidas en la Ley de 2021 se orientan a garantizar que los terroristas pasen más tiempo en prisión y a que tras su liberación pasen más tiempo bajo seguimiento. Otras muchas legislaciones han coadyuvado al fortalecimiento de la lucha contra el terrorismo. Por ejemplo, después de los ataques terroristas en Fishmongers' Hall⁶⁵² y en Streatham⁶⁵³, el

⁶⁵² El atentado de Fishmongers' Hall fue perpetrado por Usman Khan en el año 2019, quien se encontraba en libertad vigilada tras cumplir la mitad de una condena de 16 años por delitos de terrorismo. Había sido condenado en 2012 por planear la colocación de explosivos en la Bolsa de Londres y por organizar un campo de entrenamiento para terroristas en la Cachemira pakistaní. Inicialmente recibió la condena de cárcel indefinida, con un cumplimiento mínimo de ocho años. Posteriormente, tras una revisión de sentencia, se le condenó a 16 años de prisión. Cuando llevó a cabo este atentado participaba como invitado, en el marco del programa preventivo en el que participaba desde hacía años, en una conferencia organizada por la Universidad de Cambridge sobre rehabilitación de presos en el edificio Fishmongers' Hall. Con un cinturón explosivo falso adosado al cuerpo amenazó con hacer estallar su carga, antes de comenzar a apuñalar a diversas personas. El ataque ocurrió en pleno periodo electoral de Reino Unido, por lo que el endurecimiento de penas ha sido un argumento de campaña política, y tras la victoria del partido político impulsor de estas medidas, es establecieron reformas legislativas que endurecieron las condenas. Véase: «Londres llora a las últimas víctimas del terrorismo yihadista», *La Razón*, edición online de 2 de diciembre de 2019. Disponible en: <https://www.larazon.es/internacional/20191202/amliro2gfauzexjedrcnngijv.html> [Fecha de consulta: 29 de diciembre de 2023], y, «El autor del atentado de Londres participaba en una charla sobre reinserción de presos», *Heraldo*, edición online de 30 de noviembre de 2019. Disponible en: <https://www.heraldo.es/noticias/internacional/2019/11/30/la-policia-registra-la-vivienda-del-autor-del-atentado-de-londres-1346676.html> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵³ El 2 de febrero de 2020, un hombre, cuyo nombre era Sudesh Amman, efectuó un ataque con cuchillo en Streatham High Road en Streatham, Londres, antes de ser abatido por la policía. El hecho ha sido calificado como un incidente terrorista de origen yihadista. Amman estaba, en ese momento, bajo vigilancia activa contra el terrorismo, después de ser liberado recientemente de prisión después

gobierno se apresuró a poner en vigor la Ley de Delincentes Terroristas (Restricción de la Liberación Anticipada) de 2020⁶⁵⁴, que puso fin retrospectivamente a la liberación anticipada automática para todos los delincentes terroristas.⁶⁵⁵ Esta legislación de emergencia ha buscado acabar con la liberación anticipada automática a la vez que ha buscado introducir una pena de cárcel mínima de 14 años para los delitos de terrorismo. El fundamento para dicha propuesta viene dado por los últimos atentados perpetrados, previos a la implantación de la ley, por terroristas que habían sido liberados de forma anticipada y automática. Para el gobierno británico, la liberación anticipada automática suponía una modalidad de adquisición de la libertad sin control, a la que buscó poner freno, aún ante las críticas de inconstitucionalidad legislativa. Ante los hechos de controversia por la aplicación retrospectiva de esta ley, el Secretario de Justicia de entonces, Robert Buckland, ha sido tajante al expresar: "Ningún terrorista debería ser liberado anticipadamente sólo para matar y mutilar en nuestras calles. Proteger al público es el primer deber del gobierno y nuestro mensaje es claro: ya es suficiente".

En línea con esta Política Criminal, en el año 2022, a través de la Ley de Nacionalidad y Fronteras de 2022⁶⁵⁶, el gobierno revisó el Anexo 7 de la Ley contra el Terrorismo de 2000, para ampliar los poderes de la Policía Antiterrorista para que pueda aplicarse a las entradas ilegales al territorio británico, como las llegadas de retornados mediante embarcaciones pequeñas. También para evitar que personas de interés (potenciales sujetos terroristas) viajen a Reino Unido, se ampliaron los poderes de la policía de frontera aérea. Por medio del Anexo 7 de la Ley contra el Terrorismo de 2000, todos los organismos encargados de hacer cumplir la ley trabajan en estrecha colaboración y tienen mayores poderes de intervención en la frontera en servicios regulares desde fuera del Área Común de Viaje (CTA)⁶⁵⁷ para identificar cualquier problema criminal, de seguridad y de inmigración.

de una condena en 2018 por propagar material terrorista. A raíz del ataque, el gobierno británico anunció que introduciría una legislación de emergencia para evitar que los condenados por delitos terroristas fueran liberados tempranamente de la prisión. Véase: «El autor del atentado en Londres estaba bajo vigilancia tras salir de prisión», *El País*, edición online de 03 de febrero de 2020. Disponible en: https://elpais.com/internacional/2020/02/02/actualidad/1580657288_204017.html [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁴ *Terrorist Offenders (Restriction of Early Release) Act 2020*. Disponible en: <https://www.legislation.gov.uk/ukpga/2020/3/contents> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁵ «El Gobierno británico introdujo una legislación de emergencia el 11 de febrero para evitar que los condenados por terrorismo reciban una liberación anticipada automática de prisión, según un comunicado del gobierno. La legislación requerirá que los terroristas condenados se sometan a una evaluación de riesgos por parte de una junta de libertad condicional antes de optar a una salida. El gobierno apunta a aprobar la ley antes del 27 de febrero [de 2020], un día antes de que el próximo prisionero acusado por terrorismo sea liberado automáticamente. [...] La ley [que se promulgó y publicó el 26 de febrero de 2020] afectará a los actuales y futuros presos y, como tal, afectará a unos 50 presos terroristas que se encuentran actualmente en prisión. La naturaleza retrospectiva de la ley es controvertida entre los defensores de los derechos civiles y se espera que atraiga a impugnadores legales, ya que significa que los delincentes terroristas, debido a la liberación automática, tendrían que pasar más tiempo en prisión de lo que se decidió en el juicio.» Véase: «Reino Unido presenta ley de emergencia al Parlamento», *Anadolu Ajansi*, edición online de 12 de febrero de 2020. Disponible en: <https://www.aa.com.tr/es/pol/C3%ADtica/reino-unido-presenta-ley-de-emergencia-al-parlamento/1731326> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁶ *Nationality and Borders Act 2022*. Disponible en: <https://www.legislation.gov.uk/ukpga/2022/36/contents/enacted> [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁷ «El Área Común de Viajes (CTA) es un acuerdo de larga data entre Reino Unido, las dependencias de la Corona (Bailía de Jersey, Bailía de Guernsey y la Isla de Man) e Irlanda. Dicho acuerdo es anterior a la condición de miembro de Reino Unido e Irlanda a la UE. Según la CTA, los ciudadanos británicos e irlandeses pueden moverse libremente y residir en cualquiera de las jurisdicciones y disfrutar de los derechos y privilegios asociados, incluido el derecho a trabajar, estudiar y votar en determinadas elecciones, así como a acceder a prestaciones de bienestar social y servicios de salud. Los gobiernos de Reino Unido e Irlanda firmaron un Memorando de Entendimiento (MoU) en mayo de 2019 reafirmando el compromiso de mantener el CTA y los derechos y privilegios asociados, en todas las circunstancias. Al firmar el MoU, ambos gobiernos emitieron una Declaración Conjunta que está vigente hoy en día.» Véase: «Common Travel Area: rights of UK and Irish citizens Information for UK and Irish citizens on their rights under the Common Travel Area arrangements (CTA)», *Home Office*. Disponible en: <https://www.gov.uk/government/publications/common-travel-area-guidance> [Fecha de consulta: 29 de diciembre de 2023].

Cabe señalar que los poderes legales de la policía ya habían sido ampliados, concretamente en este ámbito, en el año 2017. La Ley de Policía y Crimen de 2017⁶⁵⁸ introdujo tempranamente una serie de medidas para mejorar la eficacia de las fuerzas policiales. Mediante esta Ley se creó un nuevo delito por incumplimiento de las condiciones de libertad bajo fianza, relacionadas con viajes en casos vinculados al terrorismo. Esta Ley también mejora los poderes policiales para permitir la identificación y almacenamiento indefinida de datos biométricos de una persona que tiene una condena previa en el extranjero por cualquier delito, así como dentro de Reino Unido.

En términos generales, la legislación de Reino Unido se ha ido orientando siempre hacia una mayor punición. Dicha tendencia se ha visto incrementada a partir del 11 de septiembre de 2001, por la cual la Ley contra el Terrorismo de 2000 resulta tan determinante como punto de partida a todas las reformas posteriores, o a nuevas adopciones legislativas. Con independencia de todas las leyes en materia de terrorismo que han ido aprobándose y adoptándose dentro del territorio británico, la Ley contra el Terrorismo de 2000 sigue proporcionando el marco principal para los poderes antiterroristas en Reino Unido. Contiene los principales poderes para el arresto y la detención preventiva prolongada en casos de terrorismo, así como los principales delitos de terrorismo fuera del Derecho penal común, como, por ejemplo, membresía y/o apoyo a una organización prohibida e ilegal.

Adicionalmente, la legislación de Reino Unido ha ido paulatinamente otorgando mayores facultades a sus fuerzas policiales, policía antiterrorista, unidades de inteligencia, etc., lo que ha supuesto un fortalecimiento de la estructura institucional del Estado, cuyo poder de lucha contra el terrorismo no para de crecer.

MEDIDAS DE CONTROL Y VIGILANCIA, Y REPRESIÓN CONTRA EL YIHADISMO EN INTERNET

La visión institucional de Reino Unido respecto al terrorismo es contundente, directa y sin vacilaciones. Su fundamento principal se basa en la concepción ideológica que posee el país sobre este tipo de delito. Para Reino Unido, el terrorismo no es un delito común y por ende debe ser tratado jurídica e institucionalmente atendiendo a las particularidades que lo califican como un delito de especial gravedad.

En los asuntos de seguridad interior del Estado, el terrorismo es la principal preocupación en los últimos años.⁶⁵⁹ Dentro de todas las modalidades existentes de terrorismo en Reino Unido, el terrorismo yihadista es el que mayor riesgo representa, dado que este tipo de terrorismo se observa desde hace tiempo como una amenaza duradera y cambiante,⁶⁶⁰ mientras que el

⁶⁵⁸ *Policing and Crime Act 2017*. Disponible en: <https://www.legislation.gov.uk/ukpga/2017/3/contents>. [Fecha de consulta: 29 de diciembre de 2023].

⁶⁵⁹ “La Evaluación de Riesgos de Seguridad Nacional de 2015 identificó el terrorismo como un riesgo de nivel uno, y la Revisión de Seguridad y Defensa Estratégica (SDSR) reconoció que el volumen y la escala de la amenaza en el Reino Unido y en el extranjero estaban aumentando, y que su naturaleza había cambiado.” Véase: HM GOVERNMENT (2018): *The United Kingdom’s Strategy for Countering Terrorism*, June 2018, Cm 9608, London, p. 19.

⁶⁶⁰ Se refiere principalmente al hecho de que los métodos de DAESH ya están siendo copiados por grupos terroristas nuevos.

terrorismo de extrema derecha se observa como un peligro incipiente.⁶⁶¹ En cualquier caso, para Reino Unido el terrorismo representa sin lugar a duda, a juzgar por la gran estructura institucional que posee para reprimir esta forma delictiva, una prioridad dentro de su Política Criminal de Estado.

En marzo de 2008, con el objeto de fomentar la armonización con las orientaciones europeas para luchar contra el terrorismo⁶⁶², Reino Unido publica su primera Estrategia de Seguridad Nacional (NSS): *La Estrategia de Seguridad Nacional de Reino Unido: Seguridad en un Mundo Interdependiente*.⁶⁶³

Si bien luego de haber sido publicada la misma, esta Estrategia contó con una sucesión de actualizaciones⁶⁶⁴ adaptadas a las diversas necesidades del Estado y a la creciente amenaza terrorista, la Estrategia del año 2011 merece especial atención debido a que con ella se introdujo una nueva modalidad de lucha unificada contra el terrorismo denominada *CONTEST: The UK's counter-terrorism strategy*. Dicha estrategia desarrolló y solidificó los mecanismos institucionales necesarios a fin de que el país estuviera preparado para cualquier amenaza o ante cualquier riesgo eminente de ataque terrorista. Para Reino Unido resultó adecuado entonces contar con la misma cuando, en agosto de 2014, el Centro Conjunto de Análisis del Terrorismo (*Joint Terrorism Analysis Centre, JTAC*)⁶⁶⁵ elevó el nivel de amenaza terrorista a SEVERO⁶⁶⁶, lo que significaba que era muy probable que se produjera un ataque terrorista en el país.

La estrategia CONTEST es la respuesta, por todas las vías posibles, de Reino Unido hacia el terrorismo. Pero, no es sino hasta el año 2018 cuando Reino Unido establece el mayor salto cualitativo estratégico en su lucha contra el terrorismo. La Estrategia de Seguridad del año 2018

⁶⁶¹ En el año 2016, el entonces Ministro del Interior prohibió el grupo de extrema derecha, 'Acción Nacional', en virtud de la Ley contra el Terrorismo de 2000. En el año 2017 volvió el Gobierno de Reino Unido a centrar su atención sobre el terrorismo de extrema derecha y llevó a cabo la prohibición del grupo 'Amanecer Escocés' y 'Acción Anticapitalista Nacional-socialista' que surgió como sustitución de 'Acción Nacional'.

⁶⁶² Guiadas en gran medida por la Estrategia Europea de Seguridad de 2003. Véase: CONSEJO DE LA UNIÓN EUROPEA (2003): *Estrategia Europea de Seguridad (EES, 2003): Una Europa segura en un mundo mejor*, Bruselas.

⁶⁶³ CABINET OFFICE (2008): *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, March 2008, Cm 7291, London.

⁶⁶⁴ HM GOVERNMENT (2009): *The National Security Strategy of the United Kingdom: Security for the Next Generation*, June 2009, Cm 7590, London.

HM GOVERNMENT (2010): *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, Cm 7953, London.

HM GOVERNMENT (2011a): *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, July 2011, Cm 8123, London.

HM GOVERNMENT (2012): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report*, March 2013, Cm 8583, London.

HM GOVERNMENT (2013): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report*, April 2014, Cm 8848, London.

HM GOVERNMENT (2014): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2014*, March 2015, Cm 9048, London.

HM GOVERNMENT (2015a): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2015*, July 2016, Cm 9310, London.

HM GOVERNMENT (2018), *opus cit.*

⁶⁶⁵ *Joint Terrorism Analysis Centre, JTAC*. (Centro Conjunto de Análisis del Terrorismo). Disponible en: <https://www.mi5.gov.uk/joint-terrorism-analysis-centre> [Fecha de consulta: 10 de diciembre de 2023].

⁶⁶⁶ Los niveles de amenaza terrorista de Reino Unido son cinco (BAJO: un ataque es muy poco probable, MODERADO: un ataque es posible pero no probable, SUBSTANCIAL: un ataque es probable, SEVERO: un ataque es muy probable, y CRÍTICO: un ataque es altamente probable en un futuro inminente. El nivel es fijado por el Centro Conjunto de Análisis del Terrorismo (JTAC) del Servicio de Seguridad (MI5). A diciembre de 2023, el nivel de amenaza terrorista de Reino Unido está fijado en SUBTANCIAL, según se puede observar en su página web institucional. Véase: *Terrorism and national emergencies*. (Terrorismo y emergencias nacionales). Disponible en: <https://www.gov.uk/terrorism-national-emergency> [Fecha de consulta: 10 de diciembre de 2023].

se basa en la Estrategia de Seguridad Nacional (*National Security Strategy, NSS*) y la Revisión de Seguridad y Defensa Estratégica (*Strategic Defense and Security Review, SDSR*) de 2015⁶⁶⁷, pero primordialmente atiende a los atentados del año anterior.

Los ataques terroristas en Londres y Manchester perpetrados en el año 2017⁶⁶⁸ han impulsado a Reino Unido elevar sus niveles de amenaza terrorista⁶⁶⁹ y a acrecentar sus medidas de seguridad interior y exterior dentro de su estructura institucional jurídica y policial. Estas medidas de seguridad han implicado, entre otras, la realización de una evaluación detallada e independiente, a cargo del Consejero de la Reina (*Queen's Counsel, QC*) David Anderson, del MI5 (*Security Service*)⁶⁷⁰ y la Policía Antiterrorista (*Counter Terrorism Policing, CTP*)⁶⁷¹ de los ataques en Londres y Manchester entre marzo y junio de 2017 y una revisión de mejora operacional general⁶⁷², con el objeto de identificar los “cambios operativos que deberían mejorar el desempeño futuro del MI5 y la Policía [Antiterrorista].”⁶⁷³ Todo ello hizo que los acontecimientos citados determinaran la necesidad de introducir mayores modificaciones en la estrategia CONTEST a fin de controlar potenciales riesgos tanto dentro de Reino Unido como en el extranjero.

En el año 2018, Reino Unido establece entonces una sustancial modificación a su estrategia CONTEST⁶⁷⁴ dotándola de mayores herramientas de acción en su lucha contra el terrorismo. CONTEST 2018 se focaliza en realizar una revisión, temporalmente pautada, de las amenazas del terrorismo y enfoca su estrategia antiterrorista hacia los nuevos hallazgos. De esta manera, CONTEST 2018, puede otorgar siempre la mejor y la más actualizada respuesta a la amenaza terrorista, de acuerdo con las necesidades de cada época, a la vez que establece una prospectiva en el ánimo de garantizar que Reino Unido cuente con “la mejor respuesta a la creciente amenaza en los próximos años.”⁶⁷⁵

La estrategia CONTEST, además de actualizada, es organizada e integral. Ello significa por un lado que está cimentada sobre cuatro líneas de trabajo “P” (PREVENT, PERSUE, PROTECT,

⁶⁶⁷ HM GOVERNMENT (2015b): *National Security Strategy and Strategic Defence and Security Review, A Secure and Prosperous United Kingdom*, November 2015, Cm 9161, London.

⁶⁶⁸ El atentado de Manchester del 22 de mayo de 2017 fue un ataque terrorista en modalidad suicida, en donde un hombre en solitario (‘lobo solitario’) hizo detonar a las 22:33 horas un artefacto explosivo en el vestíbulo del Manchester Arena, al término de un concierto mientras las personas se retiraban por dicho acceso. El atentado de Londres se llevó a cabo el 3 de junio de 2017 en *London Bridge y Borough Market*. Fue perpetrado a las 10:16 horas, e involucró el atropellamiento de personas con una camioneta sobre el *London Bridge*, así como el acuchillamiento de personas dentro del *Borough Market*. Ambos atentados fueron perpetrados por el autodenominado Estado Islámico (EI) según ha comunicado la propia agencia de propaganda, *Amaq*.

⁶⁶⁹ Tras el atentado terrorista en Manchester, Reino Unido eleva su nivel de amenaza terrorista al grado máximo, CRÍTICO, el cual mantuvo entre el 23 y el 27 de mayo de 2017. Véase: «Reino Unido eleva a ‘crítico’ su nivel de alerta terrorista y espera un ataque ‘inminente’ tras el atentado de Manchester», *BBC News*, edición online de 23 de mayo de 2017. Disponible en: <https://www.bbc.com/mundo/noticias-internacional-40023305> [Fecha de consulta: 10 de diciembre de 2023].

⁶⁷⁰ MI5 es como se conoce habitualmente al *Security Service* (Servicio de Seguridad), el servicio de inteligencia de Reino Unido que se dedica a la seguridad interna del Estado. Desde su creación, en el año 1909, ha funcionado bajo diferentes denominaciones: *Home Section of the Secret Service Bureau* (de octubre de 1909 a abril de 1914), *Directorate of Military Operations, section 5* [MO5]—[MO5(g)] (de abril de 1914 a septiembre de 1916), *Military Intelligence section 5* [MI5] (de septiembre a 1916 a 1929), *Defence Security Service* (de 1929 a 1931), y *Security Service* (de 1931, hasta a la fecha).

⁶⁷¹ *Counter Terrorism Policing, CTP* (Policía Antiterrorista). Disponible en: <https://www.counterterrorism.police.uk> [Fecha de consulta: 10 de diciembre de 2023].

⁶⁷² ANDERSON, David Q.C. (2017): *Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 And Police. Internal Reviews*, Unclassified, December 2017, London, pp. 1-61.

⁶⁷³ HM GOVERNMENT (2018), opus cit., p. 20.

⁶⁷⁴ *Ibidem*.

⁶⁷⁵ *Ibidem*, p. 7.

PREPARE), y por el otro, que a su vez esas líneas de trabajo integran acciones con múltiples enfoques. Las cuatro líneas de trabajo son:

«- Prevenir: impedir que las personas se conviertan en terroristas o apoyen el terrorismo.

- Perseguir: detener los ataques terroristas.
- Proteger: para fortalecer nuestra protección contra un ataque terrorista.
- Prepararse: para mitigar el impacto de un ataque terrorista.»⁶⁷⁶

Las orientaciones generales de estas líneas están recogidas en la propia estrategia. Según esta, el propósito de ‘Prevenir’ y ‘Perseguir’ es reducir las amenazas a las que Reino Unido se enfrenta; así como el propósito del trabajo de ‘Proteger’ y ‘Preparar’ es reducir las vulnerabilidades de la nación. Dentro de cada una de estas líneas se desarrollan acciones específicas orientadas a combatir el terrorismo y todas ellas poseen un enfoque multidisciplinar que une a sectores públicos y privados, comunidades, ciudadanos y socios extranjeros en torno al único propósito común de no dejar ningún espacio seguro para que los terroristas recluten o actúen. A tenor de este propósito, en el año 2018, la Primer Ministro de Reino Unido, Theresa May fue determinante, al referirse a los terroristas, al afirmar que “No se les puede permitir, ni se les permitirá tener éxito.”

CONTEST 2018 introdujo un cambio radical respecto a CONTEST 2011, y como la capacidad ampliada de investigación nacional al implementar las recomendaciones del MI5 y la revisión de mejoras operativas de CT Policing.⁶⁷⁷

Los atentados terroristas del año 2017, llevados a cabo en Londres y Manchester, han sido interpretados por Reino Unido como actos de violencia que pueden servir de motivación inspiracional para la comisión de otros ataques. Ello ha puesto el acento en la necesidad de detectar de forma temprana a personas que puedan verse motivadas por estas acciones terroristas, y por ende ser susceptibles de reclutamiento o radicalización. Debido a ello, Reino Unido comenzó a promover la necesidad de establecer un nuevo enfoque orientado a las intervenciones tempranas sobre las personas que en algún momento han sido de interés para la policía y/o las agencias de seguridad e inteligencia debido a posibles vínculos con el terrorismo. Ello ha permitido que el MI5, la Policía Antiterrorista y el Ministerio del Interior (*Home Office*) desarrollen en conjunto el Centro Multiagencia (*Multi-Agency Centre*, MAC), con el objeto de dar inicio a un nuevo modelo operativo nacional para enfrentar la amenaza terrorista. El Centro Multiagencia (MAC),

«[...] trabaja en asociación para comprender mejor el riesgo para la seguridad nacional que representan las personas que están o han estado sujetas a investigaciones de seguridad nacional, reconociendo que algunas de estas personas pueden seguir representando un riesgo.»⁶⁷⁸

⁶⁷⁶ *Ibidem*, p. 8.

⁶⁷⁷ *CT Policing* es otra forma de llamar a la Policía Antiterrorista (*Counter Terrorism Policing*, CTP).

⁶⁷⁸ Home Office in the media. Updated CONTEST strategy published. Fact Sheet: Multi-Agency Centre (MAC). Disponible en: <https://homeofficemedia.blog.gov.uk/2018/06/04/updated-contest-strategy-published/> [Fecha de consulta: 11 de diciembre de 2023].

La función de MAC se basa en reunir la experiencia existente dentro de la lucha antiterrorista, incluida la referida a ‘Prevenir y ‘Perseguir, para trabajar en asociación con expertos en gestión de delincuentes y atención social. La unión de todas estas áreas facilita el trabajo de contraterrorismo y dota de mayor capacidad para reducir el riesgo a la seguridad nacional que representan los sujetos que son prospecto de estas investigaciones.

En este contexto asociativo orientado al fortalecimiento de la seguridad nacional, la Agencia Nacional contra el Crimen (*National Crime Agency*, NCA)⁶⁷⁹ proporciona capacidad adicional a esta iniciativa institucional, al brindar información disponible de interés a la Policía Antiterrorista para trabajar de forma conjunta en áreas específicas de interés común.⁶⁸⁰

En esta línea de trabajo interinstitucional, se han desarrollado iniciativas de trabajo conjunto tendientes a proteger los espacios públicos en donde se concentra gran cantidad de personas. Ello con el afán de evitar, o dificultar, la comisión de atentados terroristas perpetrados con vehículos que son utilizados deliberadamente como armas para atropellar multitudes. Esta modalidad concreta de ataque ya ha tenido lugar en varias ciudades europeas, y en caso específico de Reino Unido los atentados de 2017 han demostrado que no solo los lugares cerrados, sino también los espacios abiertos concurridos son objetivos de ataque de los terroristas. Es precisamente tras los ataques de 2017, cuando se revisaron los enfoques existentes en este ámbito y se realizaron una serie de cambios. A fin de prevenir los ataques en lugares concurridos, cerrados y abiertos, que pueda derivar en una gran cantidad de víctimas se estableció que Asesores de Seguridad contra el Terrorismo (*Counter Terrorism Security Adviser*, CTSA) ubicados en diversas regiones del país brinden orientación de seguridad personalizada⁶⁸¹ a los propietarios y operadores de lugares concurridos y cerrados (como estadios, lugares de conciertos, discotecas, etc.). Estos miembros de CTSA a su vez imparten capacitación anual para concienciar sobre el terrorismo a un número elevado de empleados y gerentes para ayudarlos a comprender la amenaza terrorista, mejorar la seguridad de las instalaciones y reportar actividades sospechosas.

Otras alianzas público-privadas orientadas a mejorar la seguridad y a dificultar la comisión de atentados terroristas en Reino Unido, incluyen la asociación industrial conjunta del Centro Conjunto de Seguridad y Resiliencia (*Joint Security and Resilience Centre*, JSaRC)⁶⁸² y la

⁶⁷⁹ La Agencia Nacional contra el Crimen (NCA) es una agencia que ha sido creada en el año 2013 y que ayuda a perseguir y detener a delincuentes británicos miembros de organizaciones criminales y terroristas que sean difíciles de localizar y que se hayan refugiado en el extranjero. La NCA ha desarrollado un estrecho trabajo de colaboración con España dado la cantidad de ciudadanos británicos que residen en el país. Véase: «La nueva agencia contra el crimen del Reino Unido acrecienta la búsqueda de delincuentes británicos en España», *Gob.uk*, edición online de 7 de octubre de 2013. Disponible en: <https://www.gov.uk/government/news/197196.es> [Fecha de consulta: 11 de diciembre de 2023].

⁶⁸⁰ «La Policía Antiterrorista, la NCA y el Consejo de Jefes de Policía Nacional (NPCC) están implementando una estrategia de colaboración contra el terrorismo y la delincuencia grave y organizada. [Se han] identificado prioridades clave para el trabajo conjunto en áreas importantes como prisiones, inteligencia, armas de fuego y fronteras, [y se desarrollarán] nuevas iniciativas en áreas como la digital, cibernética, inteligencia y vigilancia.» Véase: HM GOVERNMENT (2018), opus cit., p. 81.

⁶⁸¹ La capacitación que brindan los Asesores de Seguridad contra el Terrorismo, a civiles propietarios de instalaciones privadas, son sobre las siguientes temas: explosivos y precursores químicos, patógenos y toxinas, fuentes radiológicas, estudio de sitios y puntos vulnerables, continuidad del negocio y recuperación ante desastres, seguridad de la información y del personal, sistemas de seguridad integrados, terrorismo por vehículos, defensa química, biológica, radiactiva o nuclear (QBRN). Véase: *Counter Terrorism Security Adviser* (CTSA). Disponible en: <https://www.police.uk/pt/contact-us/possible-terrorist-activity/contact-a-counter-terrorism-security-adviser-ctsa/?tid=911378&lid=&cid=&rid=&stepid=1> [Fecha de consulta: 11 de diciembre de 2023].

⁶⁸² «El Centro Conjunto de Seguridad y Resiliencia (JSaRC) fue fundado en 2016 por el Ministerio del Interior de Reino Unido. Forma parte del Grupo de Seguridad Nacional (HSG) y trabaja para proporcionar resultados de seguridad para Reino Unido combinando experiencia gubernamental, académica y del sector privado.» Véase: Joint Security and Resilience Centre (JSaRC). Disponible en: <https://www.jsarc.org> [Fecha de consulta: 11 de diciembre de 2023].

Autoridad de la Industria de Seguridad (*Security Industry Authority*, SIA).⁶⁸³ Esta asociación posee un gran desempeño en el desarrollo de nuevas construcciones y en remodelaciones importantes, e incorpora en sus proyectos el asesoramiento y la implementación de medidas de seguridad urbanas orientadas a la seguridad por diseño del espacio público,⁶⁸⁴ lo que resulta de gran utilidad en la prevención del terrorismo.

Este fomento de la seguridad por medio de relaciones público-privadas, Reino Unido lo desarrolla también sobre lo que denomina Infraestructura Nacional Crítica (*Critical National Infrastructure*, CNI), ello es todos los servicios y bienes inmuebles, la mayor parte de estos en propiedad privada, que son esenciales para el funcionamiento de la sociedad británica, como lo son el suministro de energía, abastecimiento de agua, transporte, salud y telecomunicaciones. Esta infraestructura crítica incluye instalaciones, sistemas, sitios, propiedades, información, personas, redes y procesos que son necesarios para mantener a Reino Unido en funcionamiento y suministrar los servicios esenciales de los que se depende. Es decir, infraestructura que, de ser interrumpida, podría tener un impacto significativo en la seguridad nacional o el funcionamiento del Estado. Por ello, la protección de la CNI contra el terrorismo es una prioridad de toda administración de gobierno.

El Centro Nacional de Seguridad Cibernética (*National Cyber Security Centre*, NCSC) y la Autoridad Nacional de Protección y Seguridad (*National Protective Security Authority*, NPSA)⁶⁸⁵ ayuda a las empresas incipientes que trabajan en tecnologías emergentes a considerar cuestiones clave en torno a la seguridad. Ambos centros brindan asesoría orientada a reducir la vulnerabilidad hacia terrorismo, principalmente frente a ataques cibernéticos. En este sentido, el NCSC trabaja muy de cerca con las fuerzas del orden y las agencias de seguridad e inteligencia para ayudar a prevenir, impedir e investigar los delitos cibernéticos y otras amenazas de índole tecnológico sobre estas infraestructuras.

En noviembre de 2016 se publicó la primera Estrategia Nacional de Ciberseguridad 2016-2021⁶⁸⁶ (*National Cyber Security Strategy 2016-2021*), que ha definido la política institucional de Reino Unido con relación a las amenazas cibernéticas que existen en el mundo digital. En el año 2022 se publicó la Estrategia de Ciberseguridad del Gobierno 2022-2030: Construyendo un sector público ciberresiliente⁶⁸⁷ (*Government Cyber Security Strategy 2022-2030: Building a cyber resilient public sector*), y en septiembre de 2023, el Ministerio de Justicia (*Ministry of Justice*, MoJ) ha publicado la segunda Estrategia de Ciberseguridad 2023-2028⁶⁸⁸ (*Cyber*

⁶⁸³ SIA es un “regulador de la industria de seguridad privada de Reino Unido. Es un organismo público ejecutivo no ministerial, patrocinado por el Ministerio del Interior.” Véase: Security Industry Authority (SIA). Disponible en: <https://www.gov.uk/government/organisations/security-industry-authority> [Fecha de consulta: 11 de diciembre de 2023].

⁶⁸⁴ La seguridad por diseño involucra el concepto y la implementación práctica de la seguridad de los edificios desde su diseño, y el rediseño de los espacios públicos atendiendo a la protección contra ataques terroristas. La seguridad por diseño se basa en los principios de proporcionalidad, multifuncionalidad, sostenibilidad, accesibilidad y estética. Es todo lo contrario a la creación de fortalezas urbanas. Véase: EUROPEAN COMMISSION. JOINT RESEARCH CENTRE (2022): *Security by Design: Protection of public spaces from terrorist attacks*. Luxembourg: Publications Office of the European Union, p. 2.

⁶⁸⁵ La Autoridad Nacional de Protección y Seguridad (*National Protective Security Authority*, NPSA) era conocida hasta hace poco como Centro para la Protección de la Infraestructura Nacional (*Centre for the Protection of National Infrastructure*, CPNI), según detalla una página web institucional. Véase: «The Centre for the Protection of National Infrastructure (CPNI) has evolved to become the National Protective Security Authority (NPSA)», *Protect UK*, edición online de 17 de marzo de 2023. Disponible en: <https://lc.cx/wpsK3U> [Fecha de consulta: 11 de diciembre de 2023].

⁶⁸⁶ HM GOVERNMENT (2016): *National Cyber Security Strategy 2016-2021*, London.

⁶⁸⁷ HM GOVERNMENT (2022a): *Government Cyber Security Strategy 2022-2030: Building a cyber resilient public sector*, London.

⁶⁸⁸ MINISTRY OF JUSTICE (2023): *Cyber Security Strategy 2023-2028*, London.

Security Strategy 2023-2028), que comprende las amenazas cibernéticas actuales y se adentra en las amenazas cibernéticas, así como en las medidas de seguridad de los futuros cinco años. La Estrategia Nacional de Ciberseguridad del año 2016 busca establecer firmemente a Reino Unido como una potencia en materia de seguridad cibernética. La Estrategia de Ciberseguridad del Gobierno del año 2022 busca garantizar que las funciones gubernamentales centrales sean resistentes a los ciberataques, fortalecer a Reino Unido y consolidarlo como una ciberpotencia. Finalmente, la Estrategia de Ciberseguridad del Ministerio de Justicia del año 2023 busca incorporar la "seguridad por diseño" en todo el Ministerio con el objeto de que la información confidencial y el trabajo judicial considerado de vital importancia este debidamente protegido y sea resistente a todo tipo de ataques cibernéticos.⁶⁸⁹

Sí bien en ninguna de las 400 páginas que abarcan las tres estrategias mencionadas, se detalla el riesgo que supone el uso de Internet con finalidad terrorista⁶⁹⁰, es reseñable el hecho que en la primera estrategia en esta materia (Estrategia Nacional de Ciberseguridad 2016-2021), se enuncie que:

«Los terroristas que utilizan Internet para sus fines no son lo mismo que el ciberterrorismo. Sin embargo, al participar cada vez más en el ciberespacio, y dada la disponibilidad de la ciberdelincuencia como servicio, uno puede dar por sentado que estarían a la medida de lanzar ciberataques.»⁶⁹¹

Este fortalecimiento de las infraestructuras críticas está orientado a prevenir e impedir un ciberataque por parte de los terroristas, dado que como la propia estrategia indica, el terrorismo está trabajando para llevar adelante acciones de mayor envergadura tecnológica, a fin de utilizar Internet para la realización de ciberataques a los Estados. Tal es incluso la prospectiva que ha desarrollado en su quinto informe anual ETL 2015, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).⁶⁹²

El último informe de ENISA, ETL 2023, que ha sido publicado en el mes de octubre de dicho año, revela que:

«Comprender al enemigo y la motivación detrás de un incidente de ciberseguridad o un ataque dirigido es importante porque puede determinar qué busca un adversario. Conocer los motivos puede ayudar a las organizaciones a determinar y priorizar qué proteger y cómo protegerlo. También proporciona una idea de las intenciones de los

⁶⁸⁹ El Servicio Nacional de Explotación Digital (*National Digital Exploitation Service*, NDES), especializado en vigilancia antiterrorista y creado en el año 2016 para abordar “*el creciente desafío que enfrenta la policía a la hora de proporcionar la evidencia digital necesaria para asegurar las condenas de los terroristas más peligrosos*,” ha expresado que una investigación terrorista típica implica aproximadamente diez terabytes de material. Véase: HM GOVERNMENT (2018), opus cit., p. 46.

Dicha información, una vez que se encuentra en dominio del Ministerio de Justicia, crece exponencialmente dado que “*utiliza una gran cantidad de hojas de cálculo, bases de datos y aplicaciones para gestionar el trabajo del departamento. El departamento tiene más de 350 terabytes de datos digitales no estructurados, procesa más de 37 millones de correos electrónicos al mes y tiene más de 100 millones de archivos, excluyendo los de los sistemas de gestión de casos*,” de ahí la necesidad imperiosa de protegerla. Véase: MINISTRY OF JUSTICE (2023), opus cit., p. 5.

⁶⁹⁰ Esto es debido principalmente al hecho de que las estrategias señaladas se centran en las vulnerabilidades tecnológicas de las instituciones del Estado, y no en los usos delictivos de las nuevas tecnologías.

⁶⁹¹ HM GOVERNMENT (2016), opus cit., p. 11 (punto 3.11).

⁶⁹² EUROPEAN UNION AGENCY FOR CYBERSECURITY (2015): ENISA Threat Landscape 2015, January 2016.

atacantes y ayuda a las entidades a centrar sus esfuerzos de defensa en el escenario de ataque más probable para cualquier activo en particular.»⁶⁹³

El panorama de ENISA en materia tecnológica, ha propiciado por parte de Reino Unido la imperiosa necesidad de fomentar una ventaja competitiva respecto de sus enemigos y posicionarse estratégicamente, dentro de la Unión Europea, como un Estado que adopta un enfoque hacia el ciberpoder.⁶⁹⁴

Sí bien el enfoque actual que posee Reino Unido respecto al uso de las nuevas tecnologías brinda gran importancia al ciberterrorismo, este país nunca ha dejado de centrar su atención en la propaganda yihadista en Internet. De hecho, Reino Unido se encuentra a la vanguardia de la lucha para abordar el contenido terrorista online, trabajando con la policía, con las empresas de tecnología, y con socios internacionales para eliminar rápidamente dicho material de Internet.

En febrero de 2010, la Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte (*Association of Chief Police Officers of England, Wales and Northern Ireland*, ACPO)⁶⁹⁵ creó la Unidad de Referencia contra el Terrorismo en Internet (*Counter-Terrorism Internet Referral Unit*, CTIRU). La Unidad de Referencia contra el Terrorismo en Internet (CTIRU), cuyo funcionamiento está a cargo de la Policía Metropolitana, se encarga de eliminar contenido de material terrorista ilegal de Internet. CTIRU trabaja con las plataformas de las principales empresas de tecnología de Internet (*Facebook*, *Twitter* -actual X-, *Google* y *Microsoft*) para identificar contenido que infringe sus términos de servicio y solicita que eliminen el contenido de forma voluntaria.

Resulta relevante mencionar el hecho de que la Unidad de Referencia contra el Terrorismo en Internet de Reino Unido (CTIRU) sirvió de base para el diseño y creación de la Unidad de Referencia de Internet de la UE de Europol (EU IRU).⁶⁹⁶ Debemos recordar que Reino Unido posee una gran tradición, en la lucha contra el terrorismo, en las alianzas público-privadas que no ha abandonado nunca, y por el contrario se ha dedicado a fortalecer con cada nueva estrategia CONTEST.

CTIRU también compila una lista de URL⁶⁹⁷ que contienen material terrorista publicado en plataformas o alojado en servidores que se encuentran fuera de Reino Unido y que no puede ser

⁶⁹³ EUROPEAN UNION AGENCY FOR CYBERSECURITY (2023): *ENISA Threat Landscape 2023*, October 2023

⁶⁹⁴ HM GOVERNMENT (2022b): *Ciberestrategia Nacional 2022: Lideramos el ciberfuturo con la participación activa de la totalidad del RU*, London, pp. 32-38.

⁶⁹⁵ La Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte (*Association of Chief Police Officers of England, Wales and Northern Ireland*, ACPO) era una sociedad sin fines de lucro que entre 1948 y 2015 lideró el desarrollo de prácticas policiales en Inglaterra, Gales e Irlanda del Norte. Durante su existencia la ACPO funcionó un foro para que los jefes de policía compartieran ideas y coordinaran sus respuestas operativas estratégicas. Entre sus actividades desarrolladas destacan el asesoramiento a gobiernos en materia de ataques terroristas y emergencias civiles, haber coordinado operaciones policiales en todo el territorio, haber desarrollado investigaciones de relevancia nacional, y haber efectuado vigilancia policial transfronteriza. Tras la denominada 'Revisión Parker' [una revisión independiente efectuada en el año 2013 que recomendó que la ACPO fuera reemplazada por un nuevo organismo] fue reemplazada en 2015, mediante la Sección 22A de la Ley de Policía de 1996 (*Section 22A, Police Act 1996*) por el Consejo de Jefes de Policía Nacional (*National Police Chiefs' Council*, NPCC).

⁶⁹⁶ "Reino Unido jugó un papel decisivo en la formación de la Unidad de Referencia de Internet de la Unión Europea (EU IRU), que entró en funcionamiento en julio de 2015, tras los ataques a *Charlie Hebdo*." Véase: «Radicalism: Internet. Question for Home Office», *UK Parliament*, edición online de 28 de junio de 2017. Disponible en: <https://questions-statements.parliament.uk/written-questions/detail/2017-06-28/1708> [Fecha de consulta: 11 de diciembre de 2023].

⁶⁹⁷ La lista CTIRU detalla las URL que por alguna razón (por ejemplo, falta de voluntad de la empresa de tecnología de Internet) no pueden o no serán eliminadas de las plataformas, de los proveedores de servicios de Internet o de motores de búsqueda. La creación

eliminados. Debido a la incapacidad para intervenir coercitivamente en la eliminación de dicho material, a modo preventivo, Reino Unido bloquea dichas URL en las redes de Internet públicas del país. De acuerdo con la estrategia CONTEST 2018, esta medida, aunada a las acciones con resultado positivo llevadas a cabo por CTIRU, han hecho que la Unidad de Referencia de Internet contra el Terrorismo de la Policía (CTIRU), “haya logrado la eliminación de más de 300.000 contenidos terroristas de Internet trabajando con la industria”⁶⁹⁸ privada.

En la actualidad, la Policía Antiterrorista y las agencias de seguridad e inteligencia tienen una variedad de capacidades tácticas y técnicas a su disposición para dismantelar la actividad terrorista, incluidas fuentes de inteligencia humana encubierta, activos de vigilancia y la interceptación legal de comunicaciones. Además de estas capacidades, también se utiliza una amplia gama de herramientas legales para limitar la capacidad de acción de los terroristas, por ejemplo, trabajando para proscribir organizaciones, congelar y confiscar sus activos financieros y dismantelar redes y asociaciones en prisión, etc. Toda capacidad institucional trabaja bajo la coordinación del “Ministro del Interior [quien] es responsable de CONTEST y cuenta con el apoyo de la Oficina de Seguridad y Contraterrorismo [(*National Counter Terrorism Security Office*, NaCTSO)] del Ministerio del Interior.”⁶⁹⁹

Adicionalmente, aparte de la estrategia CONTEST perteneciente al Estado, el Ministro del Interior asume la responsabilidad de la respuesta antiterrorista del gobierno en funciones, y se encarga de supervisar el Servicio de Seguridad (MI5) y la Agencia Nacional contra el Crimen (NCA), así como del servicio de policía en Inglaterra y Gales, y la Policía Antiterrorista (CTP).

En el año 2023, Reino Unido actualiza su Estrategia CONTEST y publica CONTEST 2023.⁷⁰⁰ En CONTEST 2023, Reino Unido, desarrolla mayores labores preventivas en el sector educativo⁷⁰¹ y en el sistema penitenciario.⁷⁰²

También se profundiza en el trabajo realizado con las empresas de tecnología para eliminar contenido terrorista y extremista violento en línea. Reino Unido ha fomentado en este aspecto también la colaboración interempresarial motivando a la industria a adoptar una posición sólida y coordinada en respuesta al terrorismo. Dichas acciones se llevaron a cabo en el Foro Global de Internet contra el Terrorismo (*Global Internet Forum to Counter Terrorism*, GIFCT)⁷⁰³ y el Llamamiento de Christchurch (Christchurch Call).⁷⁰⁴

de la lista es parte de la estrategia CONTEST desarrollada por el Gobierno como parte de su línea ‘Prevenir’. Desde 2016, todas las instituciones educativas con menores de 18 años tienen el deber legal de garantizar que sus sistemas no posean acceso a ninguno de los sitios web incluidos en la lista CTIRU. Esta lista sí bien es compilada por CTIRU, es administrada y distribuida por el Ministerio del Interior (*Home Office*) de Reino Unido.

⁶⁹⁸ HM GOVERNMENT (2018), opus cit., p. 35.

⁶⁹⁹ *Ibidem*, p. 14.

⁷⁰⁰ HM GOVERNMENT (2023): *The United Kingdom’s Strategy for Countering Terrorism*, July 2023, CP 903, London.

⁷⁰¹ Por medio de capacitación, orientación y apoyo en materia de prevención del terrorismo.

⁷⁰² Mediante el fortaleciendo de la ley y en la mejora de la capacidad institucional. Ello significa robustecer el enfoque ya existente de “separar a los reclutadores y/o radicalizadores más influyentes de la población carcelaria en general”. También mejorar el “seguimiento y gestión de los delincuentes terroristas liberados con licencia a través de nuestra nueva División de Seguridad Nacional.” Véase: *Ibidem*, p. 65.

⁷⁰³ *Global Internet Forum to Counter Terrorism* (GIFCT). Disponible en: <https://gifct.org> [Fecha de consulta: 11 de diciembre de 2023].

⁷⁰⁴ “El Llamamiento de Christchurch es un plan de acción por el que Gobiernos, Organizaciones Internacionales y actores de internet se comprometen a tomar un paquete de medidas, entre las que figuran: 1) Desarrollar herramientas para la prevención de descargas de contenido terrorista y extremista violento; 2) Luchar contra las causas del extremismo violento; 3) Mejorar la transparencia en la detección y la retirada de contenido; y, 4) Velar por que los algoritmos creados y utilizados por las compañías no orienten a los usuarios hacia contenido extremista violento para reducir su carácter viral.” Véase: «Llamamiento de Christchurch para

Entre 2018 (CONTEST 2018) y 2023 (CONTEST 2023), Reino Unido también ha trabajado en estrecha colaboración con *Tech Against Terrorism*⁷⁰⁵, con el objeto de crear una plataforma que puedan utilizar las empresas de tecnología para intercambiar su conocimiento y capacidad para prevenir el uso con fines terroristas de sus servicios.

En el desarrollo de su propia capacidad preventiva, Reino Unido continúa trabajando en su Unidad de Referencia contra el Terrorismo en Internet (CTIRU) referenciando contenido terrorista para su eliminación, y participado en los *Referral Action Days* (RADs) coordinados por Europol.

Finalmente, en un marco de colaboración internacional en materia de seguridad, Reino Unido mantiene vinculación con los EEMM de la Unión Europea, con los socios de Five Eyes (Estados Unidos, Australia, Canadá y Nueva Zelanda), con terceros Estados, con la Unión Europea (UE), Naciones Unidas (ONU) y la Organización del Tratado del Atlántico Norte (OTAN).

A su vez, en octubre de 2022, se firmó un acuerdo de intercambio de información entre Reino Unido y Estados Unidos con el objeto de asegurar que las fuerzas policiales de ambos Estados posean acceso a los datos de las empresas de tecnología de Internet. Por medio de este acuerdo se establece que todas las agencias e instituciones de Reino Unido que se encargan de luchar contra el terrorismo pueden tener acceso directo a los datos de todas las empresas proveedoras de telecomunicaciones de EEUU, y viceversa.

MEDIDAS PREVENTIVAS Y CAMPAÑAS DE INFORMACIÓN

En el año 2015, Reino Unido adoptó lo que se conoce como *Prevent duty* (Deber legal de prevención) a través de la Ley de Seguridad y Contra el Terrorismo de 2015⁷⁰⁶. Dicho ‘deber’ requiere que las autoridades locales, las escuelas, las universidades, las instituciones de educación superior, los organismos de salud, las prisiones y libertad condicional, y la policía consideren la necesidad de proteger a las personas de ser captadas por el terrorismo. Se trata de un enfoque preventivo dentro de todas las áreas que atañen a la vida de un individuo, en donde la labor de prevención de los agentes interventores o funcionarios es de carácter obligatorio y se encuentra estatuido por ley.

El Deber legal de prevención (*Prevent duty*), sí bien de desarrolla en muchas áreas, posee un interés particular dentro del ámbito educativo debido al hecho de que las instituciones educativas nuclea a un grupo etario muy susceptible a la radicalización. Por ello, proteger a los estudiantes del reclutamiento y la radicalización es parte de los deberes de protección más amplios que poseen los profesores, tutores y académicos en Reino Unido. El Deber legal de prevención (*Prevent duty*) requiere que los proveedores de educación cuenten con políticas claras para

eliminar el contenido terrorista y extremista violento de la red (15 de mayo de 2019)», *Ministère de l'Europe et des Affaires étrangères, France Diplomatie*. Disponible en: <https://www.diplomatie.gouv.fr/es/politica-exterior/diplomacia-digital/eventos/articulo/llamamiento-de-christchurch-para-eliminar-el-contenido-terrorista-y-extremista> [Fecha de consulta: 11 de diciembre de 2023].

Este plan de acción es desarrollado por una comunidad de más de 130 gobiernos del mundo, empresas de tecnología de Internet, Organizaciones Internacionales y organizaciones de la sociedad civil que con una actuación conjunta buscan eliminar el contenido terrorista y extremista violento online. Véase: *Christchurch Call*. Disponible en: <https://www.christchurchcall.com> [Fecha de consulta: 11 de diciembre de 2023].

⁷⁰⁵ *Tech Against Terrorism*. Disponible en: <https://techagainstterrorism.org/home> [Fecha de consulta: 11 de diciembre de 2023].

⁷⁰⁶ Véase: *Security and Counter-Terrorism Act of 2015* (Ley de Seguridad y contra el Terrorismo de 2015). Disponible en: <https://www.legislation.gov.uk/ukpga/2015/6/contents/enacted> [Fecha de consulta: 29 de diciembre de 2023].

proteger a los estudiantes y desarrollar su resiliencia a la radicalización en las escuelas y las instituciones de educación superior y superior.

En este ámbito, la red de Oficiales de Educación Preventiva⁷⁰⁷ desempeña un papel clave para el desarrollo de esta labor al brindar apoyo a las escuelas en áreas prioritarias por su mayor riesgo de reclutamiento y/o radicalización terrorista, y al informar sobre el desarrollo de políticas y prácticas que se implementan a nivel nacional.

Para apoyar a las escuelas, el Departamento de Educación y el Ministerio del Interior de Reino Unido desarrollaron conjuntamente un sitio web llamado ‘Educar contra el odio’ (*educate.against.hate*) que ofrece a profesores, líderes escolares y padres toda la orientación y el apoyo que necesitan para proteger a sus hijos de la radicalización y el extremismo.⁷⁰⁸ El sitio web también incluye consejos sobre cómo mantener a los niños a salvo de las influencias extremistas en línea.

Cabe señalar que el enfoque preventivo orientado como una vía de solución a los problemas, no resulta novedoso para el Estado británico, dado que considerar la peligrosidad del terrorismo en materia preventiva se suma a las obligaciones establecidas a los profesionales, desde hace mucho tiempo, de proteger a las personas vulnerables de una variedad de daños, como drogas, pandillas y explotación física y sexual. El ‘deber’, en el caso concreto del terrorismo, está diseñado para ayudar a garantizar que las personas vulnerables que se encuentran en riesgo de radicalización reciban el apoyo que recibirían en procesos similares de protección en los que ya se viene trabajando desde hace décadas.

En la Estrategia CONTEST 2018⁷⁰⁹, en el marco de las cuatro líneas de trabajo “P” (PREVENT, PERSUE, PROTECT, PREPARE), se detalla extensamente este enfoque. Es precisamente en la estrategia *Prevent*⁷¹⁰, en donde se desarrollan orientaciones específicas a fin de “impedir que las personas se conviertan en terroristas o apoyen el terrorismo.”⁷¹¹ Además, Reino Unido también asume las orientaciones de la Unión Europea en este sentido, y, al igual que la Unión, entiende que los terroristas utilizan narrativas para justificar comportamientos que contradicen y socavan los valores de cualquier sociedad democrática. Dichas narrativas tienden a fragmentar y dividir las comunidades europeas por medio de la difusión de fundamentalismos violentos que suelen ser la antesala de los atentados terroristas. En respuesta a ello, el enfoque *Prevent* tiende a proteger el Estado de derecho, la libertad individual, la democracia, el respeto mutuo, la

⁷⁰⁷ *Prevent Education Officer (PEO)*. El Oficial de Educación Preventiva (PEO) es una persona designada que se encuentra en cada institución educativa de Reino Unido y que tiene la responsabilidad de apoyar a las escuelas en todas las etapas clave de la formación de los estudiantes, así como apoyar a todo el personal dentro de las instituciones educativas, con el objeto de identificar vulnerabilidades y riesgos de índole terrorista. El PEO posee un papel crítico en el desarrollo de una buena conciencia política porque habitualmente se encarga también de realizar actividades de capacitación a fin de aumentar el nivel de conciencia de los estudiantes y de reducir el riesgo de reclutamiento y/o radicalización de estos. Para esta capacitación se suelen utilizar los paquetes *Prevent* de formación para escuelas (*WRAP training materials*), que se encuentran disponibles en formato electrónico y de forma online, que incluyen estudios de casos relacionados con la radicalización islamista y de extrema derecha, y brindan información sobre mecanismos de apoyo y prevención. También se utiliza la Guía sobre el Deber legal de prevención (*Prevent Duty Guidance*), que es una orientación específica para las autoridades de Inglaterra y Gales sobre el deber establecido en la Ley de Seguridad y Contra el Terrorismo de 2015 acerca de la exigencia de evitar que las personas se vean arrastradas hacia el terrorismo.

⁷⁰⁸ El Departamento de Educación y Ministerio del Interior de Reino Unido han desarrollado un sitio web en donde se facilitan todas estas herramientas preventivas de aplicación específica en el sector educativo. Véase: *Educate.against.hate, Department for Education and the Home Office, UK*. Disponible en: <https://www.educateagainsthate.com/prevent-training/> [Fecha de consulta: 29 de diciembre de 2023].

⁷⁰⁹ HM GOVERNMENT (2018), *opus cit.*

⁷¹⁰ HM GOVERNMENT (2011b): *Prevent Strategy*, June 2011, Cm 8092, London.

⁷¹¹ HM GOVERNMENT (2018), *opus cit.*, p. 8.

tolerancia y la comprensión de las diferentes religiones y creencias, combatiendo el extremismo con una estrategia preventiva que tiende a intervenir en la primera fase, o fase ideológica, del terrorismo.

El enfoque estratégico *Prevent* de la Estrategia CONTEST contrarresta las ideologías terroristas abordando las causas de la radicalización. A priori se identifica que la radicalización es un proceso complejo, de carácter individual y en el que no interviene un factor único. En términos generales, el extremismo se orienta a la promoción del odio, la erosión de los derechos de grupos específicos, la propagación de la intolerancia y el aislamiento de las comunidades. La estrategia *Prevent* se orienta específicamente a intervenir en comunidades vulnerables o susceptibles a procesos de radicalización yihadista. Sí bien el área comunitaria del programa es opcional (el área institucional, que abarca a centros educativos, hospitales, centros de menores, etc., es obligatoria a todos los funcionarios involucrados), se ha detectado que las comunidades que no participan o no pueden participar tienen más probabilidades de ser vulnerables a la radicalización. De ahí que se deduzca que una estrategia de integración (institucional y comunitaria) exitosa es importante para la lucha coordinada en la prevención contra el terrorismo.

El propósito central de *Prevent* es salvaguardar y apoyar a las personas vulnerables para evitar que se conviertan en terroristas o que apoyen el terrorismo. El trabajo de *Prevent* también se extiende más allá de los límites anticipatorios y brinda apoyo para la rehabilitación y reinserción social de quienes ya están involucrados en el terrorismo. *Prevent* funciona de manera similar a los programas diseñados para proteger a las personas de las pandillas, el abuso de drogas y el abuso físico y sexual. El éxito preventivo en esta materia está dado en el hecho de que se centra concretamente en abordar las causas de la radicalización, y en eliminar aquellos factores que potencian dicho riesgo.

La intervención preventiva se realiza de forma presencial en las diferentes comunidades, y de forma virtual en línea. Y en ambos casos la orientación es la misma, brindar apoyo continuo y eficaz a quienes son vulnerables a la radicalización, y promover la retirada de quienes ya participan en el terrorismo o quienes lo apoyan buscando la rehabilitación de dichos sujetos. A todo efecto y en todo Reino Unido, los objetivos de *Prevent* son:

«1) Abordar las causas de la radicalización y responder al desafío ideológico del terrorismo, 2) Salvaguardar y apoyar a quienes corren mayor riesgo de radicalización mediante una intervención temprana, identificándolos y ofreciéndoles apoyo, y, 3) Permitir que aquellos que ya han participado en el terrorismo se retiren y se rehabiliten.»⁷¹²

No obstante, las investigaciones gubernamentales y académicas han indicado consistentemente que no existe un perfil sociodemográfico único de un terrorista en el Reino Unido, ni una única vía o camino que conduzca a su participación en el terrorismo; de ahí que, aunque la estrategia *Prevent* posea los mismos objetivos para todo Reino Unido, no se aplica de igual forma en todo el Estado, de modo que se ajusta en cada caso a las particularidades de las comunidades locales de cada sitio y/o región.

⁷¹² *Ibidem*, p. 31.

Cabe señalar también que los terroristas provienen de una amplia gama de orígenes y parecen involucrarse en las actividades terroristas de diferentes maneras y por diferentes razones. No existe un único factor que por sí solo haga que alguien se involucre en el terrorismo. Habitualmente varios factores pueden converger para crear las condiciones propicias bajo las cuales puede tener lugar un proceso de radicalización. Estos factores de fondo suelen ser aspectos propios o inherentes a las circunstancias personales de alguien que podrían hacerlo vulnerable a los reclutadores o radicalizadores, como por ejemplo estar involucrado en actividades delictivas, poseer influencias, ideas o experiencias previas que influyan u orienten a apoyar un movimiento terrorista, ser propenso a adoptar una ideología extremista.⁷¹³

Internet es una poderosa herramienta que los terroristas explotan para radicalizar, preparar y reclutar a personas vulnerables, e incitar a la comisión de ataques terroristas. Los grupos terroristas hacen un uso extensivo de diferentes plataformas en línea para comunicarse con miles de personas y difundir su ideología y propaganda. En este sentido, Reino Unido adopta no solo las medidas institucionales que tienden a impedir la difusión de contenido terrorista en línea, sino que mediante la estrategia *Prevent* promueve una respuesta preventiva que se basa en trabajar con grupos de la sociedad civil para desarrollar su capacidad de cuestionar y contrarrestar las narrativas terroristas en línea. Dicho trabajo se realiza mediante campañas de concienciación y por medio de grupos o referentes legitimados en la sociedad.

La *Research, Information and Communications Unit* (Unidad de Investigación, Información y Comunicaciones (RICU))⁷¹⁴ ayuda a estos grupos o referentes a amplificar sus voces tanto de forma presencial en las comunidades, así como principalmente de forma online mediante el uso de Internet. RICU se encarga de que estos grupos y/o referentes legitimados socialmente que serán la voz o cara de las campañas de prevención contra el reclutamiento y/o radicalización del terrorismo, accedan a apoyo digital, asesoramiento creativo, capacidades de producción, creación de sitios web, capacitación en medios y asesoramiento en relaciones públicas.

Prevent funciona principalmente bajo un estricto análisis de amenazas que desarrolla Reino Unido en su territorio. Con los resultados de estos análisis se establece una dirección única pero conjunta, entre RICU y cada autoridad local. Esto quiere decir que la estrategia *Prevent* está en gran medida dirigida localmente y que esta dirección se apoya en el análisis de la amenaza concreta que se cierne sobre cada comunidad específica. RICU opera centralmente formando una red preventiva con las autoridades locales.

⁷¹³ HM GOVERNMENT (2011b), opus cit., pp. 23-25.

⁷¹⁴ La Unidad de Investigación, Información y Comunicaciones (*Research, Information and Communications Unit, RICU*) se estableció en 2007 bajo el capítulo *Prevent* de la Estrategia *CONTEST* del HMG (HM GOVERNMENT). Además de desarrollar la contranarrativa gubernamental, RICU proporciona un análisis sobre el uso terrorista de la propaganda y la explotación de Internet por parte del yihadismo para luego informar al sistema antiterrorista de Reino Unido. Para respaldar este objetivo crucial, RICU lleva a cabo un monitoreo de código abierto para comprender mejor el entorno de los medios, en línea y de las comunicaciones en relación con el terrorismo y el extremismo. Este monitoreo de código abierto identifica una variedad de material que se comparte y discute dentro de estos espacios, incluidos temas o medios que grupos terroristas y extremistas buscan explotar. Toda la recopilación y análisis de datos de RICU cumple con la legislación vigente británica. Los ministros han autorizado el trabajo de RICU desde su creación en 2007 y mediante actualizaciones posteriores de la estrategia *CONTEST* (en 2011, 2018 y 2023) y reciben periódicamente los resultados de RICU. El trabajo de RICU es crucial para la ejecución de *Prevent* y ha ayudado a posicionar a Reino Unido a la vanguardia de la batalla contra la propaganda terrorista, particularmente el contenido terrorista en línea. Véase: HAYES, Ben/ QURESHI, Asim (2016), opus cit.

El Deber legal de prevención (*Prevent duty*) requiere que, dentro de esta red de trabajo de la estrategia *Prevent*, las autoridades locales establezcan o hagan uso de grupos multiinstitucionales existentes para evaluar la situación local, coordinar actividades y establecer acuerdos para monitorear el impacto del trabajo preventivo. En las áreas prioritarias donde se considera que el riesgo de radicalización es mayor, los coordinadores de *Prevent* empleados por las autoridades locales crean asociaciones con entidades referentes en las comunidades, supervisan la ejecución de planes de acción locales para responder al riesgo de radicalización, y trabajan para incorporar actividades de prevención en los estatutos de los servicios públicos y privados de atención social, salud y educación.

Dentro de la Guía sobre el Deber legal de prevención (*Prevent Duty Guidance*), se establece que sí un funcionario público o un trabajador de primera línea tiene alguna inquietud acerca de una persona, dentro de la institución en la cual se desarrolla habitualmente, sobre la que cree que podría ser vulnerable a la radicalización, puede remitirlo o referirlo dentro de la propia institución para que reciba el apoyo o intervención adecuada.⁷¹⁵ Esta acción se conoce como Referencias de *Prevent* (*Prevent referrals*).⁷¹⁶

Además, el público en general puede hacer referencias a su autoridad o a la policía local mediante la campaña ACT (*Action Counters Terrorism: Acción Contra el Terrorismo*)⁷¹⁷. La campaña ACT, llevada a cabo por la Policía Antiterrorista de Reino Unido, busca alentar a los ciudadanos a estar atentos a actividades y/o comportamientos sospechosos de terrorismo y reportarlos a la policía.⁷¹⁸ La primera campaña de ACT generó un aumento del 55 % en las llamadas a la línea directa antiterrorista de la policía y un mayor nivel de conciencia poblacional sobre a qué prestar atención para identificar posibles radicalizaciones y prevenir actos de terrorismo.

En el caso de que se considere que una persona es vulnerable a la radicalización, se le puede ofrecer apoyo a través del programa *Channel* en Inglaterra y Gales, o el programa *Prevent Multi-Agency Panel (PMAP)* en Escocia⁷¹⁹. “Se trata de programas interinstitucionales diseñados para salvaguardar y apoyar a personas vulnerables que corren el riesgo de verse arrastradas al terrorismo”.⁷²⁰ El programa *Channel*⁷²¹ se gestiona en todas las autoridades locales de Inglaterra y Gales⁷²² y aborda todo tipo de extremismo, incluidos los de extrema derecha y los relacionados con el islamismo.

⁷¹⁵ Existen mecanismos de protección aplicables en primer lugar para abordar dichas inquietudes, y muy a menudo pueden gestionarse de manera interna y sin derivaciones posteriores a autoridades policiales.

⁷¹⁶ «Guidance: Making a referral to Prevent», *GOV.UK*. Disponible en: <https://www.gov.uk/guidance/making-a-referral-to-prevent> [Fecha de consulta: 29 de diciembre de 2023].

⁷¹⁷ *Action Counters Terrorism* (ACT). Disponible en: <https://act.campaign.gov.uk> [Fecha de consulta: 29 de diciembre de 2023].

⁷¹⁸ ACT (*Action Counters Terrorism*) ofrece todo tipo de medio de contacto para reportar una actividad sospechosa: por medio de un formulario online, por medio del teléfono 0800 789 321, y también posee un número telefónico de asistencia prioritaria (número de teléfono 999) en caso de que el reporte sospechoso requiera un tratamiento de emergencia. Además, cuenta con el programa *ACT Early*, que está especialmente dirigido a familiares o allegados de alguna persona que está siendo manipulada por el terrorismo a fin de brindar asesoramiento y ayuda inmediata para evitar una potencial radicalización de alguien afectivamente cercano.

⁷¹⁹ *Prevent Multi-Agency Panel (PMAP)* anteriormente tenía el nombre de *Prevent Professional Concerns* (PPC).

⁷²⁰ HM GOVERNMENT (2018), *opus cit.*, p. 38.

⁷²¹ «Channel Program», *GOV.UK*. Disponible en: <https://www.gov.uk/government/publications/channel-and-prevent-multi-agency-panel-pmap-guidance> [Fecha de consulta: 29 de diciembre de 2023].

⁷²² *Prevent* se desarrolla a través de servicios delegados dentro del gobierno de Gales

Para aquellas derivaciones en las que la policía evalúa que existe riesgo de radicalización, una junta local de *Channel* –que está presidido por la autoridad local y compuesto por representantes de diferentes áreas de protección, incluidas la salud, la educación y la policía⁷²³– se reunirá para discutir cada caso y evaluar el alcance de la vulnerabilidad potencial del individuo. En caso de que el individuo posea un alto riesgo o vulnerabilidad se le brinda apoyo. Este apoyo consiste en proveer educación o empleo, servicios de salud, asesoría, o tutoría ideológica para proporcionar a las personas vulnerables las habilidades para protegerse de actividades relacionadas con el terrorismo o de apoyar el terrorismo.

La participación en el programa *Channel* es totalmente voluntaria. Las personas deben otorgar su consentimiento para recibir el apoyo. En caso de que un individuo decida abandonar el programa antes de tiempo, se pueden acceder a formas alternativas de apoyo por parte de la autoridad local u otros socios locales⁷²⁴. En caso de que un sujeto no acceda a participar en el programa *Channel* o en caso de abandonar el programa antes de tiempo, el riesgo terrorista que ello supone es gestionado entonces directamente por la policía.

Para Fatima Lahnait, el programa *Channel* representa el “componente esencial de la estrategia Prevent de Reino Unido, la cual se creó ya en 2003, aunque no se anunció públicamente hasta años más tarde como parte de la estrategia antiterroristas amplia denominada CONTEST.”⁷²⁵ Si bien en términos generales para esta autora la Estrategia CONTEST y sus derivados resultan óptimos, cabe, según ella, la crítica por una posible estigmatización del colectivo musulmán por su origen y/o religión. Adelantándose a esta posible valoración, Reino Unido desarrolló en el marco contextual de *Prevent*, estrategias que no solo tiendan a prevenir el terrorismo y/o la radicalización sino también a prevenir las visiones prejuiciosas y/o los discursos de odio amparados en un radicalismo de derechas orientado hacia la comunidad musulmana. Nace así, la RADEQUAL⁷²⁶, una campaña que ha tenido su nacimiento en Manchester y que se orienta a repensar la radicalización mediante un análisis que permite identificar y entender cuáles son las preocupaciones y los desafíos que deben enfrentar las diferentes comunidades y las diferentes situaciones de tensión y/o divisiones en sus comunidades en forma de odio, prejuicio y/o extremismo. RADEQUAL se orienta también a crear una red de líderes de opinión legitimados que pueda minimizar los efectos de dichas tensiones, así también como promover la inclusión y las sanas diferencias.⁷²⁷

Asimismo, y siguiendo las orientaciones de la Unión Europea en este sentido, en el año 2016 el alcalde de Londres Sadiq Khan, desarrollo una campaña denominada *#LondonisOpen* (Londres

⁷²³ Entre ellos, representantes de centros de enseñanza, trabajadores sociales, presidentes de juntas locales de protección de la infancia, etc.

⁷²⁴ Existen muchas organizaciones sin ánimo de lucro que desde hace años colaboran para crear una mejor convivencia comunitaria. Un ejemplo es el grupo *London Tigers* (*London Tigers Football Club* es un club de fútbol con sede en Greenford, en el distrito londinense de Ealing) que ha estado durante años incentivando a miembros de grupos delincuenciales a acercarse al club mediante un sentido de hermandad deportiva. A partir del establecimiento de la estrategia *Prevent*, *London Tigers* desarrolló un nuevo enfoque acorde al programa *Channel*, a fin de acercarse a los grupos vulnerables susceptibles de reclutamiento y radicalización con la intención de brindar un lugar de encuentro deportivo que permita aunar la identidad religiosa propia con la pertenencia nacional. Véase: PROCTOR, Natalia (2019): «Anti-Radicalisation. Report 2019», *Counter Terrorism Preparedness Network (CTPN)*, First edition, London Resilience Group, (1-54), p. 19.

⁷²⁵ LAHNAIT, Fatima (2021), opus cit., p. 52.

⁷²⁶ RADEQUAL. Disponible en: <https://www.manchester.gov.uk/makingmcrcsafer/info/6/work/6/radequal-rethinking-radicalisation-programme> [Fecha de consulta: 29 de diciembre de 2023].

⁷²⁷ PROCTOR, Natalia (2019): «Anti-Radicalisation. Report 2019», *Counter Terrorism Preparedness Network (CTPN)*, First edition, London Resilience Group, (1-54), p. 18.

es abierta)⁷²⁸. Dicha campaña se orientó a promover la cohesión entre las diferentes comunidades⁷²⁹, así también como entre diferentes ciudadanos de la Unión Europea residentes en Reino Unido. Con esta iniciativa se buscó reducir la intolerancia, el odio y la polarización de pensamiento. En todo tipo de formatos audiovisuales (cartelería, páginas webs, folletos, videos turísticos promocionales, etc.), discursos, publicidad institucional, etc., se buscó introducir diferentes lemas⁷³⁰ alusivos al hecho de que Londres es una ciudad inclusiva.⁷³¹

Estas medidas de cohesión social e inclusión son también modelos preventivos para hacer más evidente (por falta de integración, violencia y/o rechazo hacia los países europeos) la identificación de aquellas personas que por diversos motivos se adhieren al terrorismo.

Además de las campañas orientadas a identificar posibles sospechosos de actividad terrorista y de campañas de cohesión social, en Reino Unido se ha desarrollado una variedad de campañas de contranarrativa. En el marco de estas campañas preventivas orientadas a desarrollar un contradiscurso, es reseñable la actividad de Quilliam.⁷³² Quilliam ha sido un *think tank* británico que ha cesado sus funciones en el año 2020 debido a las dificultades que enfrentó su financiación

⁷²⁸ *London Is Open*. Disponible en: <https://www.london.gov.uk/london-open> [Fecha de consulta: 29 de diciembre de 2023].

⁷²⁹ Según la estrategia Prevent, “un sentido más fuerte de ‘pertenencia’ y ciudadanía hace que las comunidades sean más resistentes a la ideología terrorista y a los propagandistas. Creemos que Prevent depende de la integración, la participación democrática y un fuerte diálogo interreligioso.” Véase: HM GOVERNMENT (2011b), opus cit., p. 27.

⁷³⁰ Algunos de ellos han sido: “Dignity has no nationality” (La dignidad no posee nacionalidad), “Everyone welcome” (Todos bienvenidos), “No them only us” (No ellos, solo nosotros), “Work towards world peace” (Trabajar por la paz mundial), “We are all londoners” (Todos somos londinenses), etc.

⁷³¹ Orientaciones similares a esta campaña las podemos encontrar en otras ciudades importantes de Europa, como Madrid. La presidente de la Comunidad de Madrid, Isabel Díaz Ayuso, en reiteradas ocasiones se ha referido en comparecencias al “*Madrid de todos*”, y ha expresado: “*todos quieren venir a conocernos, ser un madrileño más y expresar la vida con alegría e intensidad*”. Además, la Comunidad de Madrid “*ha dado a conocer que, en el primer semestre de 2024, un nuevo portal web disponible en diez idiomas además de español (inglés, francés, alemán, italiano, portugués, chino, coreano, japonés, ruso y árabe) integrará la agenda turística de todos los municipios a través de las últimas tendencias tecnológicas.*” Estas declaraciones y acciones pueden observarse fácilmente como una búsqueda de posicionamiento turístico, pero responden también a las orientaciones europeas acerca de promover una visión ideológica que fomente la cohesión social y minimice las tensiones sociales. Véase: «Díaz Ayuso invita a conocer la Comunidad de Madrid ‘al servicio de España’ con ‘el mejor escenario cultural que nadie pueda imaginar’», *Portal de la Comunidad de Madrid*. Disponible en: <https://www.comunidad.madrid/noticias/2024/01/26/diaz-ayuso-invita-conocer-comunidad-madrid-servicio-espana-mejor-escenario-cultural-nadie-pueda-imaginar> [Fecha de consulta: 26 de enero de 2024].

⁷³² Quilliam fue creado en 2007 por Ed Husain, Majid Nawaz y Rashad Zaman Ali, todos ex miembros del grupo islamista *Hizb ut-Tahrir**. La organización inicialmente llevaba el nombre de Abdullah Quilliam, un ciudadano británico del siglo XIX que se convirtió al Islam y que fundó la primera mezquita de Gran Bretaña. La organización también se llamó Quilliam y (antes de su cierre) The Quilliam Foundation. Su página web <http://www.quilliamfoundation.org> se encuentra actualmente (periodo 2023/2024) en desuso. Dicha web fue consultada por mi persona en reiteradas ocasiones entre 2016 y 2019. [* “*Hizb ut-Tahrir al Islami (Partido de la Liberación Islámica) es un movimiento social muy activo en Europa, Asia Central y Oriente Próximo. En el Líbano, uno de los pocos países del mundo árabe donde es legal (junto con Yemen y Emiratos Árabes Unidos), ha rechazado entrar en la contienda electoral, pero no a participar activamente en la vida política del país a través de su movimiento social que ellos llaman ‘partido’*”. *Hizb ut-Tahrir al Islami (Partido de la Liberación Islámica)*, deriva de Hizb ut Tahrir Al Quds (Partido de la Liberación de Jerusalén). “*Hizb ut Tahrir Al Quds (Partido de la Liberación de Jerusalén) nació en 1953 para liberar a Jerusalén de la ocupación sionista. Pero su fundador, Taqiuddin al-Nabhani, amplió pronto sus objetivos para buscar la liberación de los musulmanes de la cultura dominante, de la modernidad occidental, que es para ellos un cáncer que amenaza la supervivencia del propio islam. Pasaron así a llamarse Hizb ut Tahrir al Islami (Partido de la Liberación Islámica) y pronto se vieron obligados a pasar a la clandestinidad. En más de medio siglo, Hizb ut Tahrir se ha ido transformando y adaptando a las circunstancias. En los años sesenta y setenta participó en actos de lucha armada y se vio, supuestamente, envuelto en intentos de golpe de Estado (Taji-Farouki, 1996)*1. Después, pasó a ser muy activo en el ámbito social, pero sin entrar en competición con el resto de partidos políticos de los países en los que se encontraba presente. Su estrategia, establecida por al-Nabhani, contempla tres pasos (adoctrinamiento, interacción y toma del poder) y, al menos en la letra, ha sido mantenida por sus líderes posteriores (Abdul Qadim Zallum y Ata Abu Rashta). Su primer objetivo no es lograr un cambio político inmediato, sino transformar la sociedad (especialmente las élites) a través de una revolución cultural, ya que la política es sólo un epifenómeno de la cultura, un simple producto de esta.” Léase: ALONSO MARCOS, Antonio (2011): «Hizb ut Tahrir en el Líbano: Sus aportaciones al islam político», *Revista CIDOB d’Afers Internacionals*, núm. 93-94, (201-217), p. 202. El objetivo final del *Hizb ut-Tahrir* (Partido de la Liberación Islámica) es el de establecer un califato mundial. En enero de 2024 *Hizb ut-Tahrir* fue oficialmente declarado grupo terrorista y ha pasado a engrosar la lista de organizaciones prohibidas en Reino Unido. Véase: Nota a pie de página N.º 598.

gubernamental planteadas por el Covid-19. Durante los años que estuvo en funcionamiento, obtuvo un gran protagonismo en Reino Unido por sus actividades de diseminación de narrativas (en diversos formatos audiovisuales⁷³³) orientadas a deslegitimar el mensaje yihadista en Internet. Sin embargo, a pesar de la popularidad alcanzada, este *think tank* no estuvo exento de polémica, dado que para un segmento de la población que profesa el islam, Quilliam

«pretende, entre otras muchas actividades, desafiar las narrativas violentas abogando por relatos alternativos plurales y democráticos. [...] No obstante, su labor ha sido fuertemente discutida por la comunidad islámica británica por los vínculos y el asesoramiento que la fundación mantiene con el gobierno.»⁷³⁴

Durante sus años de ejercicio, Quilliam o Quilliam Foundation, ha promovido una visión no violenta del islam (yihadismo) en Reino Unido, pero no del extremismo islámico. Esto, que en principio puede parecer confuso, tiene su lógica en los objetivos de los fundadores de Quilliam que han seguido sosteniendo los valores ideológicos de *Hizb ut-Tahrir* (Partido de la Liberación Islámica) dentro de Quilliam. Es decir, Quilliam durante muchos años ha trabajado en Reino Unido como el *think tank* musulmán que rechaza los métodos violentos del yihadismo, pero no la ideología extremista del islam.

Por su rechazo directo al yihadismo, Quilliam ha sido duramente criticado. Tanto ha sido así que “el décimo cuarto número de la revista *Dabiq*, difundido el 12 de abril de 2016, ilustra en un artículo titulado ‘*Kill the Imams of Kafr in the West*’⁷³⁵, su beligerancia con los musulmanes tildados de apostatas que viven en Occidente y que socaban el relato yihadista”⁷³⁶.

Paradójicamente, Quilliam ha llevado a cabo de forma online y presencialmente en Reino Unido y en otros países de Europa diversos trabajos discursivos que en algún sentido han apoyado los discursos extremistas. La base de su contradiscurso ha sido siempre atacar el yihadismo y la

⁷³³ “Entre sus múltiples propuestas resalta un desafío creativo llamado Openyoureyes mediante el cual anima a grabar [a la población] cortometrajes sobre temáticas relacionadas con la narrativa violenta y sus alternativas.” Véase: TOBOSO BUEZO, Mario (2016), opus cit., p. 8. Nota adicional: la cita textual se refiere a un período (año 2016, según fecha de la publicación) en el que el *think tank* aún existía, de ahí que el autor se exprese en tiempo presente.

⁷³⁴ *Ibidem*.

⁷³⁵ “Mata a los Imanes de Kafr en Occidente.”

Kafir (no *Kfar*, como en alguna ocasión se ha indicado) es una contracción de la palabra árabe *Kafir* “otro”. El concepto del ‘otro’ dentro del movimiento político-religioso de ISIS ha sido abordado en numerosas ocasiones en las revistas *Dabiq* y *Rumiyah*, planteando la idea de que ‘los otros’ (es decir, aquellos que no están vinculados a la ideología yihadista) son traidores. Sí bien los artículos, que hacen referencia a la otredad, está redactados en inglés, los mismos “están plagados de términos árabes, especialmente cuando se hace referencia a aquellos que son considerados enemigos o aquellos que no son verdaderos creyentes en la versión de la fe de ISIS” [...] Este proceso de instaurar la idea de otredad “fue central no solo para el fundamento teológico, sino también para la organización. Creo una afilada distinción basada en el ‘nosotros-ellos, que tenía como objetivo aumentar el sentido de pertenencia dentro de la comunidad de ISIS” [...] “Quizás la palabra más común de un ‘otro’ para ISIS es *kafir*.” *Kafir* es cualquiera que se desvíe de la interpretación del islam que hace el movimiento yihadista. El término también puede transcribirse como *kafir*, *kaffar* o *karif*” [...] “Etimológicamente el término proviene de la raíz K-F-R que se refiere a los agricultores que plantan semillas en el suelo y las cubren con tierra. Por analogía, [para el yihadismo] un *kafir* oculta la verdad o se oculta de la verdad, ya sea mediante un acto de desvío o de indiferencia.” En el léxico de ISIS, *kafir* se aplica prácticamente a “cualquiera que desconoce o rechaza el islam.” [...] No obstante, son los imanes saudíes los peormente señalados. El término que utiliza ISIS para ellos es *murtad*, que significa apóstatas, “una palabra aplicada a personas que fingen ser musulmanas, pero no son verdaderos creyentes.”

En el artículo referenciado, que lleva por título ‘*Kill the Imams of Kafr in the West*’ y que ha publicado *Dabiq*, se dice que los imanes saudíes son sin duda *murtaddin*. Y que “su apostasía es aún más flagrante que cualquier otra, habiendo estudiado el texto claro que demuestra su colapso en *kafr*.” Véase: JUERGENSMEYER, Mark (2022): «Othering in ISIS», en: JUERGENSMEYER, Mark (Ed.)/ MOORE, Kathleen (Ed.)/ SACHSENMAIER, Dominic (Ed.), *Religious Othering: Global Dimensions*, London: Routledge, (111-122), p. 115-117.

⁷³⁶ TOBOSO BUEZO, Mario (2016): opus cit.

utilización de los métodos violentos aplicables a su ideología, pero no necesariamente a su ideología.

En diciembre de 2016, durante la asistencia a un Workshop organizado por el Ayuntamiento de Málaga, se tuvo la oportunidad de contemplar en primera persona el trabajo de Quilliam en España.⁷³⁷ En dicha ocasión, en el transcurso del primer día, y en el marco de las exposiciones de los ponentes Adam Deen⁷³⁸, Nikita Malik y el jeque Dr. Usama Hasan, se detalló la distinción entre extremismo y radicalización. Conforme a estos ponentes, existe una clara diferencia entre ambos conceptos debido a que “el extremismo genera la promoción de una interpretación y de una visión del islam”, que “puede ser violenta o no”, y que “construye un discurso monofocal”. Por el contrario, en la radicalización “el ‘otro’ es deshumanizado”, por lo tanto “implica necesariamente violencia”, y respecto al sujeto radicalizado se expuso que se trata de un “individuo con crisis de identidad (real o autopercebida) que es “vulnerable a los mensajes de radicalización”. Los ponentes, todos ellos miembros de Quilliam, indicaron que el *think tank* trabajaba sobre el individuo, “construyendo mensajes que ataquen dicha vulnerabilidad” a fin de que los musulmanes con una visión extremista del islam abandonasen la violencia como método. Sin embargo, además de establecer dicha distinción, se rescató la idea de que el discurso extremista, desde su concepción ideológica, “posee siempre un componente de verdad para que sea aceptado”. Habida cuenta de que los fundadores de Quilliam, han sido y son miembros de *Hizb ut-Tahrir* (Partido de la Liberación Islámica), cuyo objetivo final es establecer un califato mundial, no ha pasado desapercibido el hecho de que las visiones extremistas (no violentas) del islam sean observadas con tanta benevolencia y que se haya promovido cierta legitimación de ellas desde un *think tank* que ha funcionado gracias a la financiación gubernamental británica.

Ya se trate de iniciativas privadas o estructuras preventivas públicas, Reino Unido continúa apostando por la labor preventiva de la Estrategia CONTEST, y la aplicación específica de la estrategia *Prevent* y el programa *Channel*. Entre 2016 y 2017, se publicaron las primeras estadísticas que recogían los datos de 2015, y se contabilizó que un total de 6.093 personas fueron remitidas a *Prevent*. De ellos, el 45% declararon de forma voluntaria requerir algún tipo de apoyo alternativo, el 36% no requirió ningún apoyo adicional, y un 19% de casos se discutieron en juntas locales del programa *Channel*. De este 19%, 332 personas recibieron apoyo del *Channel* y un 79% de ellas abandonaron el proceso al haber sido evaluado que no presentaban más preocupaciones relacionadas con el terrorismo.

En el año que finalizó el 31 de marzo de 2023, hubo 6.817 derivaciones a *Prevent*, un aumento del 6,4 % en comparación con el año anterior y el tercer total más alto de derivaciones desde 2015. Este aumento no se tradujo en más casos de intervención del programa *Channel*, ya que solo se adoptaron 654 derivaciones, 159 menos que el año anterior. La mayoría de las derivaciones (39%) provinieron del sector Educación, seguido de la policía con el 29% del total. Los niños y jóvenes están excesivamente representados en los datos de *Prevent* y *Channel*, con un 63% de las referencias relacionadas con menores de 20 años y un 31% con 14 años o menos.

⁷³⁷ POLÍTICAS Y COMUNICACIÓN ESTRATÉGICA PARA LA PREVENCIÓN DE LA RADICALIZACIÓN VIOLENTA. (*Workshop*). Programa dirigido a profesionales, investigadores y Fuerzas y Cuerpos de Seguridad. Organizado por Ayuntamiento de Málaga, Área de Derechos Sociales, y Escuela de Seguridad Pública del Ayuntamiento de Málaga (ESPA) y Quilliam, 1 y 2 de diciembre de 2016, Málaga, España.

⁷³⁸ Ex miembro de *Al Qaeda* y participe ideológico y material en el ataque a las Torres Gemelas del 11 de septiembre. (Según testimonio de participación y la propia declaración de membresía del ponente).

También hubo un mayor número de remisiones relacionadas con preocupaciones de terrorismo de extrema derecha (19%) en comparación con el extremismo islamista (11%), cuya tendencia de remisiones disminuye a lo largo de los años.⁷³⁹

Reino Unido ha emprendido una lucha contra el terrorismo desde hace ya muchos años que ha ido perfeccionando a base de legislación, experiencia, colaboración público-privada, instituciones específicas de antiterrorismo, y su estrategia CONTEST, así como sus modelos preventivos. Legislativamente ha sido avanzada en la adopción de legislación específica antiterrorista con una clara orientación hacia el Derecho penal del enemigo. El sistema institucional de Reino Unido ha ido centrándose poco a poco en un modelo con amplias medidas tendientes a la securitización del Estado, como unidades de inteligencia, policías, funcionarios de fronteras, etc. Destaca en este segmento la *Counter-Terrorism Internet Referral Unit* (Unidad de Referencia contra el Terrorismo en Internet, CTIRU), cuyo trabajo ha inspirado la EU IRU (Unidad de Referencia de Internet de la Unión Europea), y la *Research, Information and Communications Unit* (Unidad de Investigación, Información y Comunicaciones, RICU). El modelo preventivo se desarrolla en torno a la estrategia *Prevent*. Dentro de la estrategia *Prevent* podemos encontrar un enfoque mixto que tiende a orientar su trabajo desde un punto de vista punitivo (*Prevent duty*), correctivo (Funcionarios públicos que referencian, *Channel*) y mecánico (CTIRU y RICU). Lo interesante del modelo es que no trabaja de forma colaborativa entre las partes, dado que no hay partes que unir. *Prevent* es un modelo preventivo que se desarrolla en las áreas descritas pero que trabaja al unísono dado que dentro de su estrategia considera todos los campos de acción. Aunque la estrategia *Prevent* tenga especial protagonismo, no debemos de olvidar que la misma se encuentra enmarcada en una estrategia mayor radicular que es la Estrategia CONTEST. La Estrategia CONTEST promueve la eliminación del terrorismo en Reino Unido por todos los medios posibles. Este posicionamiento hace que su Política Criminal respecto al terrorismo yihadista adhiera al *Warfare*.

Tabla 5: Medidas de la Política Criminal de Reino Unido respecto al delito de terrorismo.

TERRORISMO	ALEMANIA	REINO UNIDO	ESPAÑA
Derecho Penal	Derecho penal del ciudadano	Derecho penal del enemigo	
Sistema Institucional	P/CEV	CONTEST	
Modelo Preventivo	Mixto (punitivo, correctivo, mecánico)	<i>Prevent</i>	
Tendencia de la Política Criminal	Lawfare	Warfare	

Fuente: Elaboración propia. 2023.

⁷³⁹ «New statistics show increase in Prevent referrals», *Counter Terrorism Policing*. Disponible en: <https://www.counterterrorism.police.uk/new-statistics-show-increase-in-prevent-referrals/> [Fecha de consulta: 29 de diciembre de 2023].

CAPÍTULO 10: ESPAÑA

LA POLÍTICA CRIMINAL DE ESPAÑA EN MATERIA DE TERRORISMO

La experiencia de España en la lucha contra el terrorismo, protagonizado en el ámbito nacional por organizaciones como ETA o GRAPO, le ha permitido estar al país en una posición adelantada en la elaboración de legislación para la persecución de este delito. Esto ha marcado notablemente su Política Criminal con relación al terrorismo, que ha estado caracterizada por una visión tendiente a la erradicación total de este crimen.

El mayor exponente de la Política Criminal española con relación al terrorismo ha sido su legislación en la materia. A lo largo de los años, el desarrollo normativo ha sido muy profuso y ha estado sometido a constantes modificaciones orientadas permanentemente a la erradicación de este delito en todas sus formas.

La Ley del 10 de julio de 1894 determinó el inicio de una Política Criminal de carácter punitivo que se orientó principalmente a la represión de las corrientes anarquistas de fines del siglo XIX. La orientación temprana de esta Política Criminal con relación a este delito estuvo en gran parte determinada por la colaboración recibida en ese entonces por parte de la Alemana nazi. En 1941, Heinrich Himmler, jefe de las SS, y sus consejeros delegados viajaron a España para instruir en materia de seguridad de Estado y en ordenación policial.⁷⁴⁰

En este mismo año se establece la Ley de Policía y con ella se fundamenta jurídicamente la creación de la Brigada Político Social, una policía secreta, especializada y política encargada de mantener el orden público durante la época del franquismo y la transición.⁷⁴¹

Durante esta época se aprueba el Código Penal de 1944 donde, en su artículo 260, se recoge la tipificación del delito de terrorismo. La tipificación que se realiza de este delito es en exceso vaga y describe como terrorismo un peligro abstracto contra la seguridad del Estado, y que se castiga con pena de reclusión perpetua o muerte, incluso en los supuestos en donde no se hubieren conseguido los efectos pretendidos o no hubiere mediado la utilización de explosivos.⁷⁴² La tipificación del artículo 260 del CP de 1944 resulta tan amplia que, según Mestre Delgado, dicha disposición se utilizaba también para reprimir cualquier forma de delincuencia sin relación alguna con el terrorismo, manteniendo los mismos criterios de pena.⁷⁴³ Esta situación tenía lugar porque la finalidad de todas las instituciones policiales de la época se centraba en luchar no solo contra el terrorismo, sino también contra toda forma de disidencia social.

⁷⁴⁰ «El jefe de las SS visita España», *El País*, edición online de 15 de octubre de 2015. Disponible en: https://elpais.com/elpais/2015/10/13/fotorrelato/1444747453_605541.html [Fecha de consulta: 22 de diciembre de 2022].

⁷⁴¹ La Brigada Político Social “fue uno de los pilares fundamentales de la represión del franquismo. Pero también del mantenimiento del orden público durante los años de la Transición y posteriormente. Porque, aunque este Cuerpo se disolvió en 1978, sus miembros y métodos siguieron actuando.” Véase: «La Secreta de Franco: ya era hora de investigar a la Brigada Político Social», *Conversaciones sobre Historia*, 21 de abril de 2022. Disponible en: <https://conversacionsobrehistoria.info/2022/04/21/la-secreta-de-franco-ya-era-hora-de-investigar-a-la-brigada-politico-social/> [Fecha de consulta: 22 de diciembre de 2022].

⁷⁴² REINARES NESTARES, Fernando/JAIME-JIMÉNEZ, Oscar (2000): «Countering terrorism in a new democracy: the case of Spain», en: REINARES NESTARES, Fernando (Ed.), *European democracies against terrorism: governmental policies and intergovernmental cooperation*, Ashgate, p. 133.

⁷⁴³ MESTRE DELGADO, Esteban (1987): *Delincuencia terrorista y Audiencia Nacional*. Madrid: Centro de publicaciones del Ministerio de Justicia.

En 1974 tiene lugar una mayor actividad terrorista en España y debido a ello se implementan cambios en los aparatos de seguridad del Estado. En 1975 se reforma la Dirección General de la Guardia Civil para agilizar la lucha contra el terrorismo, y se incrementa el número de policías uniformados, encubiertos y antidisturbios.⁷⁴⁴ En 1975, por medio del Decreto-Ley 10/1975⁷⁴⁵, tiene lugar un nuevo endurecimiento de la normativa en materia de terrorismo. Por medio de este decreto se reducen garantías, se elevan las penas, se aumenta la clasificación de actividades terroristas, se amplía el plazo para poner a un detenido a disposición judicial, y el plazo de prisión provisional. Este Decreto-Ley introducía por vez primera el delito de enaltecimiento del terrorismo. Es reseñable este hecho habida cuenta de que esta tipificación es precisamente uno de los usos propagandísticos que realiza actualmente el yihadismo en Internet. El artículo 10 del Decreto-Ley 10/1975 enunciaba:

«[...] Los que, públicamente, sea de modo claro o encubierto, defendieren o estimularen aquellas ideologías a que se refiere el artículo cuarto de esta disposición legal; o el empleo de la violencia como instrumento de acción política o social; o manifestaren su aprobación o pretendieren justificar la perpetración de cualquier acto terrorista; o enaltecieron a sus ejecutores o participantes [...] serán castigados con la pena de prisión menor, multa de cincuenta mil a quinientas mil pesetas e inhabilitación especial para el ejercicio de funciones públicas y para las docentes, públicas o privadas.»

Es reseñable que hasta 1977 coexistían en España dos ordenamientos jurídicos para el tratamiento de los delitos de terrorismo: el derecho común (art. 260 del CP) y el Código de Justicia Militar (art. 294 bis a., b. y c.). No obstante, esto cambia con las primeras elecciones democráticas celebradas tras la finalización del régimen franquista, y el 5 de enero de 1977 se crea la Audiencia Nacional⁷⁴⁶ y a partir de aquí los delitos de terrorismo pasan a ser competencia exclusiva de la Audiencia Nacional, y los artículos 294 bis a., b. y c. pertenecientes al Código de Justicia Militar se integran ahora al Código Penal español.

En este nuevo escenario democrático, se busca como primera medida reducir la injerencia del Ejército en asuntos de orden público interno. Se realizan por tanto muchos cambios de índole constitucional, y entre otras medidas se suprime la Brigada Político-Social⁷⁴⁷ que era parte de la organización del entonces denominado Cuerpo Superior de Policía (CSP).

Este cambio orgánico fue el primero de muchos que realizó España en un periodo que se caracterizó por desarrollar mayor legitimidad jurídica. Este periodo, aunque supuso una gran cantidad de garantías y adopciones constitucionales dentro de la Política Criminal española, no ha tenido injerencia alguna en la legislación existente y/o futura para la lucha contra el terrorismo.

Un ejemplo de ello es el Decreto-Ley 21/1978⁷⁴⁸. Este Decreto-Ley supone la primera normativa redactada en democracia y resulta particular porque revela que aún en un Estado de Derecho, con relación a los delitos de terrorismo España mantendrá ciertos criterios punitivos y

⁷⁴⁴ *Ibidem*.

⁷⁴⁵ Decreto ley 10/1975, de 26 de agosto, sobre prevención del terrorismo.

⁷⁴⁶ Real Decreto-ley 1/1977, de 4 de enero, por el que se crea la Audiencia Nacional.

⁷⁴⁷ «Posible "desmilitarización" de la Policía Armada», *El País*, edición online de 8 de junio de 1977. Disponible en: https://elpais.com/diario/1977/06/08/espana/234568804_850215.html [Fecha de consulta: 22 de diciembre de 2022].

⁷⁴⁸ Real Decreto-ley 21/1978, de 30 de junio, sobre medidas en relación con los delitos cometidos por grupos o bandas armadas.

comenzará a legislar en esta materia conforme el Derecho penal de excepción.⁷⁴⁹ A partir de este momento tienen lugar una gran variedad de modificaciones al CP existente, y nuevas adopciones que se caracterizará por mantener la misma tendencia legislativa del derecho de excepción.

En 1978 se adopta la Ley 56/1978, de 4 de diciembre que se centra en la tipificación de los delitos de terrorismo cometidos por “personas integradas en grupos organizados y armados.”⁷⁵⁰ Días después, también en el mes de diciembre, se modifica la materia de terrorismo dentro del Código Penal mediante la Ley 82/1978⁷⁵¹. Mediante esta ley se modifican, se suprimen y se introducen nuevos artículos a fin de lograr más precisión en la tipificación. En 1979 se adopta el Real Decreto-ley 3/1979, sobre Seguridad Ciudadana⁷⁵² que provee un tratamiento acorde a todo lo mencionado previamente. Por medio de este Real Decreto-ley se amplía la incomunicación del detenido hasta 10 días, se faculta a registros domiciliarios sin necesidad de autorización u orden judicial, y se autoriza la intervención telefónica y postal. El Real Decreto-ley de 1979 reconoce por vez primera en España al terrorismo como una conducta delictiva diferenciada de cualquier otra forma de delincuencia. Por otra parte, a su vez, en este Real Decreto-ley se determina la necesidad de introducir en el Código Penal la tipificación detallada del delito de apología del terrorismo.

En 1980 entra en vigor la Ley Orgánica 11/1980, de 1 de diciembre.⁷⁵³ La LO 11/1980 busca subsanar en gran medida la discutible legitimidad formal de las medidas antiterroristas de los últimos años, así por medio de esta nueva legislación la incomunicación del detenido pasa de 10 días a un máximo de 72 horas desde su detención, surge el derecho a la inviolabilidad de domicilio sin consentimiento o resolución judicial, y el derecho a la inviolabilidad de las comunicaciones. Cabe señalar que esta LO 11/1980 generó un gran debate político previo a su aprobación con motivo de que establecía la definición de una nueva política legislativa.

En 1981, también en una búsqueda de establecer una Política Criminal diferente en el ámbito del terrorismo, se introduce en el Código Penal, mediante la Ley Orgánica 2/1981⁷⁵⁴, la figura del arrepentido. En el artículo 174 bis, c), de la LO 2/1981 se recoge que:

«El integrante, colaborador o cooperador de los grupos o bandas armadas que espontáneamente coadyuvare con las Fuerzas de Seguridad o con la Autoridad Judicial con actos suficientes para evitar la comisión del delito o aminorar sus efectos, o aporte pruebas definitivas para la identificación o la captura de los partícipes, se le rebajará en dos grados la pena que le correspondiera por su participación en dichos delitos.»

⁷⁴⁹ Conforme a lo expresado por Francisco Muñoz Conde, el Derecho penal de excepción es un tipo de derecho que “*claramente se opone al modelo de Estado democrático*”, y resulta “*difícilmente compatible con los principios y bases del Estado de Derecho*.” Se caracteriza según el autor por una concepción autoritaria del Derecho penal. Este Derecho penal de excepción o Derecho penal del enemigo es muy característico de los “*regímenes totalitarios de Hitler, Mussolini, Stalin o Franco, o en las dictaduras del Cono Sur americano (Argentina, Chile, Uruguay, Paraguay, Brasil) durante los años 70*”. Sin embargo, una vez finalizados estos regímenes, ello tiene lugar también en los Estados democrático de Derecho. Véase: MUÑOZ CONDE, Francisco (2011), opus cit., p.127.

⁷⁵⁰ Ley 56/1978, de 4 de diciembre, de medidas especiales en relación con los delitos de terrorismo cometidos por grupos armados. (art. 1).

⁷⁵¹ Ley 82/1978, de 28 de diciembre, de modificación del Código Penal en materia de terrorismo.

⁷⁵² Real Decreto-ley 3/1979, de 26 de enero, sobre protección de la seguridad ciudadana.

⁷⁵³ Ley Orgánica 11/1980, de 1 de diciembre, sobre los supuestos previstos en el artículo 55, 2, de la Constitución.

⁷⁵⁴ Ley Orgánica 2/1981, de 4 de mayo, que modifica y adiciona determinados artículos del Código Penal y el de Justicia Militar.

Sin embargo, estos cambios durarían poco tiempo. En 1984 se adopta la Ley Orgánica 9/1984⁷⁵⁵, de 26 de diciembre. Mediante esta LO se busca el endurecimiento de las medidas contra el terrorismo dentro del Estado español. Esta LO fue duramente criticada por la cantidad de preceptos constitucionales que infringía. Entre otras cosas, se equiparaba en determinados supuestos la autoría a la participación (arts. 7, 8 y 9), volvía a prolongar hasta diez días la detención policial (art. 13), se podía decretar la incomunicación del detenido “por el tiempo que se considere necesario” (art. 15), se facultaba al ingreso domiciliario sin consentimiento u orden judicial (art. 16), se volvía a autorizar la intervención de comunicaciones, postal, telegráfica y telefónica por plazos de 3 meses prorrogables (art. 17), se autorizaba el cierre de medios de comunicación conforme a actuaciones del Ministerio Público (art. 21), y otras modificaciones.

Todo ello significaba naturalmente un regreso a la Política Criminal que tradicionalmente se había llevado adelante en materia de terrorismo en España. Debido a ello tuvo lugar en 1987, la Sentencia del Tribunal Constitucional⁷⁵⁶ a partir de los recursos de inconstitucionalidad planteados por el Parlamento Vasco y el Parlamento de Cataluña contra el contenido de la Ley Orgánica 9/1984.

Con motivo del fallo emitido en la STC 199/1987 y las críticas que dichas modificaciones establecieron en gran parte de la sociedad española, así también como en la comunidad académica y jurídica, en 1988 se produce una nueva reforma en el CP que se realiza por medio de la adopción de la LO 3/1988⁷⁵⁷, de 25 de mayo. Por medio de la LO 3/1988 se deroga la LO 9/1984, de 26 de diciembre. Estos hechos de avance y retroceso constitucional de la legislación terrorista es para Cano Paños parte de las “contradicciones del Estado constitucional, el cual, impotente para mantenerse fiel a sus genuinas señas de identidad garantista, ha caído y sigue cayendo en la provocación terrorista, procediendo a dinamitar alguna de las más importantes conquistas jurídico-penales del siglo XX.”⁷⁵⁸

En 1991 se establece en España el denominado régimen FIES⁷⁵⁹ (Fichero de Internos de Especial Seguimiento), por medio de Circular de 6 de marzo de 1991. Para los internos bajo el régimen FIES, ello se traducía en mayores medidas de vigilancia y control. Según González Collantes. para los internos FIES se requerían:

«[...] informes diarios relativos a los cacheos practicados, a las actitudes de los internos, a las relaciones con otros internos e incidentes producidos, se ordenaban cambios de celda semanales, inspecciones oculares nocturnas al menos cada hora, o que no hubiera internos FIES en celdas contiguas, etc.»⁷⁶⁰

⁷⁵⁵ Ley Orgánica 9/1984, de 26 de diciembre, contra la actuación de bandas armadas y elementos terroristas y de desarrollo del artículo 55.2 de la Constitución.

⁷⁵⁶ Sentencia del Tribunal Constitucional 199/1987, 16 de Diciembre de 1987.

⁷⁵⁷ Ley Orgánica 3/1988, de 25 de mayo, de Reforma del Código Penal.

⁷⁵⁸ CANO PAÑOS, Miguel Ángel (2008b): «Los inicios de la lucha antiterrorista en Alemania. Análisis de la legislación penal y procesal en las décadas de 1970-1980», *Revista Electrónica de Ciencia Penal y Criminología* (en línea), núm. 10-14, pp. 1-31.

⁷⁵⁹ Base de datos de carácter administrativo que almacena información sobre determinadas personas internadas en centros penitenciarios.

⁷⁶⁰ GONZÁLEZ COLLANTES, Talía (2014): «Los ficheros de internos de especial seguimiento: un ejemplo de la penetración de la cultura de emergencia y la excepcionalidad en el ámbito penitenciario», *Revista Pensamiento Penal*, 11 de agosto, Asociación Pensamiento Penal, pp.1-16.

Dicha circular detalla también la creación de los FIES-RE (régimen especial), orientado a todos los internos que hubieren cometido delitos de terrorismo o los considerados especialmente peligrosos.

Años más tarde, en 1995, tiene lugar la adopción de una nueva legislación, la Ley Orgánica 10/1995⁷⁶¹, de 23 de noviembre, de Código Penal. Hasta la fecha no había alusión alguna a la comisión de delitos de terrorismo por medio de Internet.

El conocimiento que ha brindado el estudio del terrorismo nacional, caracterizado por su profusa normativa, le ha permitido a España identificar a los grupos terroristas como organizaciones cuya estructura se erige cohesionada alrededor de uno o varios líderes, orgánicamente definida mediante el reparto estanco de roles y funciones, y con estrictas relaciones de jerarquía. Sí bien, en el caso de ETA, por ejemplo, la organización había sufrido modificaciones en su estructura, la característica que predominaba era la centralización.

La información acerca de cómo se estructuraba una organización terrorista otorgaba mucha certeza a la hora de categorizar y clasificar el terrorismo como tal. Es decir, durante muchos años en España, las organizaciones terroristas no eran tal solo por el cometido criminal de sus acciones, sino también por las características de su estructura interna que facilitaba la identificación de los grupos terroristas habida cuenta de los aparatos internos de una organización. Y ese conocimiento, a su vez, facultaba a promover una legislación *ad hoc* en la materia a fin de recoger en normativa penal española qué es y cuáles son las características de un grupo terrorista.

Sin embargo, para el año 2006, ETA establece un cambio en su estructura interna por motivos de seguridad. Los procedimientos de investigación desarrollados de forma colaborativa entre Francia y España entre 1996 y 2006 orientados al desmantelamiento de la estructura de ETA, promovieron en la organización un cambio sustancial, y “ETA ha reaccionado disminuyendo la centralización y dispersando las responsabilidades en muchas más manos”.⁷⁶² Ello significa que de estar organizada tradicionalmente en cinco aparatos ha pasado a once aparatos.⁷⁶³

Sí bien ETA desarrolla una vertiente internacional, la misma resulta exigua comparada con el terrorismo global actual propio del yihadismo. Y sí bien la nueva organización interna de ETA es significativa por cuanto ha llevado a los Fuerzas y Cuerpos de Seguridad de España a tener que aprender el funcionamiento de una nueva estructura más descentralizada, esto no supera los límites del conocimiento planteado hasta entonces porque no ha habido cambios dentro de la tipificación penal del delito de terrorismo en cuanto a la descripción de grupo terrorista, y por ello se mantenía dentro de lo previsible.⁷⁶⁴

⁷⁶¹ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

⁷⁶² «ETA ha modificado su estructura interna por motivos de seguridad», *El Correo*, 23 de marzo de 2006. Disponible en: https://www.elcorreo.com/vizcaya/pg060323/actualidad/politica/200603/23/ECD_eta_funcionamiento.html#&ref=https://www.elcorreo.com/vizcaya/pg060323/actualidad/politica/200603/23/ECD_eta_funcionamiento.html [Fecha de consulta: 22 de diciembre de 2022].

⁷⁶³ Estos once aparatos que componen formalmente, para el año 2006, la nueva estructura de ETA es: logística, política, internacional, militar, reserva, makos (cárceles), extorsión, información, reclutamiento (captación), negociación y tesorería.

⁷⁶⁴ Se alude al cambio en el organigrama que tiene lugar del terrorismo local o nacional al terrorismo global del yihadismo. En donde se parte de una estructura, más o menos centralizada para comenzar a tratar con un esquema global de terrorismo, completamente descentralizado y con infinidad de “lobos solitarios”.

Este cambio de estructura del terrorismo implicó para España no solo un nuevo conocimiento, sino incluso un nuevo aprendizaje sobre la marcha. Para el 2000, tal era la información sobre el terrorismo de ETA, y tal el desconocimiento del terrorismo yihadista, que cuando tuvo lugar el 11-M en Madrid dicho atentado fue atribuido inicialmente, tanto por el gobierno como por medios de comunicación, al grupo terrorista ETA.

Aunque sí bien es cierto que se conocieron posteriormente motivaciones políticas para atribuir la autoría a ETA, y negar en principio la existencia de otro tipo de terrorismo, es cierto también que la presencia mediática de este grupo terrorista en la sociedad española facilitó este argumentario. Debido a ello, durante los primeros días posteriores al atentado, los medios de comunicación enfatizaron en la idea de la autoría de ETA sobre los atentados, aun a pesar de que Fuerzas y Cuerpos de Seguridad del Estado, y áreas operativas internas de estos, barajaban otras hipótesis. A propósito de este hecho, Juan Jesús Sánchez Manzano, el jefe de los TEDAX en el año 2004, declaraba:

«La obsesión de estos periodistas [se refiere a Pedro J. Ramírez, Casimiro García-Abadillo y Federico Jiménez Losantos, periodistas del periódico El Mundo] fue tal que, ya publicadas las sentencias de la Audiencia Nacional (2007) y del Tribunal Supremo (2008), en junio de 2009 seguían insistiendo en la autoría de la banda criminal ETA.»⁷⁶⁵

Dicha situación motivó una investigación que supuso la apertura mediática a difundir a la sociedad española la existencia de una nueva forma de terrorismo dentro del Estado, caracterizada por ser transnacional y de etiología religiosa. Esto supuso una ruptura a todo nivel, ya que significó posicionarse estableciendo adecuaciones a la Política Criminal de entonces. En el siguiente inciso se analizará en detalle cómo a partir de este terrorismo global, la Política Criminal española con relación al terrorismo se ve influenciada por las medidas adoptadas por la Unión Europea, a fin lograr una armonización en esta materia.

LAS MEDIDAS DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA CON RELACIÓN AL TERRORISMO YIHADISTA EN INTERNET ADOPTADAS EN LA POLÍTICA CRIMINAL ESPAÑOLA

INSTRUMENTOS NORMATIVOS PARA LA PERSECUCIÓN DEL TERRORISMO ONLINE

Considerando la Resolución 2178 del Consejo de Seguridad de Naciones Unidas, aprobada el 24 de septiembre de 2014, en donde se pone de manifiesto una profunda preocupación por parte de la comunidad internacional en vista del recrudecimiento de la actividad terrorista, especialmente la concerniente al terrorismo internacional yihadista, y por la intensificación del llamamiento a la comisión de atentados en diversas partes del mundo, los Estados del Sistema internacional comenzaron a establecer modificaciones en sus disposiciones penales a fin de adecuarlas a las nuevas formas de los delitos de terrorismo internacional.

⁷⁶⁵ «Apoyo a los TEDAX de la Policía Nacional», *Revista 11Magina*, edición online de diciembre 2023, Año XIII, N.º 23. Disponible en: https://asociacion11m.org/wp-content/uploads/2023/11/IIMAGINA-23_WEB.pdf [Fecha de consulta: 22 de diciembre de 2022].

El terrorismo internacional de índole yihadista se identifica como un nuevo fenómeno caracterizado por haber incorporado nuevas formas de agresión, consistentes en la utilización de un nuevo instrumento para la captación, adiestramiento y adoctrinamiento en el odio. El nuevo instrumento al cual se hace referencia es Internet, que comienza a observarse como un espacio virtual que debe ser regulado conforme facilita la perpetración de estos nuevos delitos. El nuevo terrorismo se caracteriza por su vocación de expansión internacional, por medio de líderes carismáticos que difunden consignas y mensajes por medio de Internet, haciendo uso de redes sociales y plataformas web específicas. En este nuevo escenario de terrorismo global España tempranamente busca alinearse a las recomendaciones de la ONU y primordialmente a las recomendaciones de la Unión Europea, con el objeto de adecuar su legislación para luchar más eficazmente contra esta nueva modalidad de terrorismo dentro de su propio territorio.

Como ya hemos observado, la legislación española en materia de terrorismo ha sufrido múltiples modificaciones y las mismas siempre han atendido a la experiencia del ámbito interno. La inclusión de Internet como elemento constitutivo de delito por parte del nuevo terrorismo yihadista, suscita un cambio legislativo que evidencia el salto de un terrorismo local (ETA) a uno internacional (Al Qaeda y Dáesh).

Se establece por tanto la modificación de la Ley Orgánica 10/1995⁷⁶⁶ en materia de delitos de terrorismo, mediante la aprobación y sanción de la Ley Orgánica 2/2015, de 30 de marzo. En el ámbito de esta experiencia de adecuaciones legislativas, el Código Penal español mantiene una tradición de respuesta penal de excepción, pero ampliando ahora su comprensión del terrorismo a una contextualización moderna y adaptada a las amenazas actuales, a fin de dar cabida a conductas de terrorismo de tipo individual⁷⁶⁷ y a las actuales acciones terroristas orientadas a la propaganda en Internet que al presente constituyen la principal preocupación internacional.

El 30 de marzo de 2015 tuvo lugar la aprobación de la Ley Orgánica 2/2015, en materia de delitos de terrorismo.⁷⁶⁸ La LO 2/2015 incorpora, en torno a la tipificación, nuevos delitos de terrorismo (consistentes en la captación, radicalización y adiestramiento) cuya consideración nace a partir de las propuestas de la UE. Adicionalmente se establecen modificaciones en el enfoque político-institucional al denominar a través de esta normativa al terrorismo como un “asunto prioritario de Estado.”⁷⁶⁹ Esta sutil pero significativa modificación que implementa España está en consonancia con los criterios europeos para enfrentar la lucha contra el terrorismo en Europa y en cada país de la Unión.

1. Análisis comparativo entre la Ley Orgánica 10/1995, de 23 de noviembre, y la Ley Orgánica 2/2015, de 30 de marzo

1.1 En relación con la tipificación del delito de terrorismo:

⁷⁶⁶ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

⁷⁶⁷ Preámbulo de Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁷⁶⁸ Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁷⁶⁹ DIARIO LA LEY (2015), opus cit.

En el caso de la LO 10/1995, de 23 de noviembre, el delito de terrorismo se encuentra descrito en los artículos del 571 al 580 del Código Penal. Por medio de la LO 10/1995, de 23 de noviembre se interpreta el delito de terrorismo como delito contra el orden público.

Conforme a lo expuesto en el art. 572 de la LO 10/1995, de 23 de noviembre, son terroristas:

«los que perteneciendo, actuando al servicio o colaborando con bandas armadas, organizaciones o grupos cuya finalidad sea la de subvertir el orden constitucional o alterar gravemente la paz pública, cometan los delitos de estragos o de incendios tipificados en los artículos 346 y 351, respectivamente,... [y] ...serán castigados con la pena de prisión de quince a veinte años, sin perjuicio de la pena que les corresponda si se produjera lesión para la vida, integridad física o salud de las personas».

La Ley Orgánica 2/2015, de 30 de marzo, introduce una nueva definición de terrorismo que se encuentra inspirada en la Decisión Marco 2002/475/JAI. La definición establece en su artículo 573 que la comisión de cualquier delito grave enumerado en el inciso 1 del artículo, constituye un delito de terrorismo, cuando se llevase a cabo con cualquiera de las finalidades siguientes:

«art. 573.1.1 Subvertir el orden constitucional o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo; art. 573.1.2 Alterar gravemente la paz pública; art. 573.1.3 Desestabilizar gravemente el funcionamiento de una organización internacional; 573.1.4 Provocar un estado de terror en la población o en una parte de ella.»

El concepto de terrorismo se encuentra definido en ambos casos por medio de la finalidad y las acciones criminales, no obstante, en la LO 10/1995, de 23 de noviembre, aun es necesario recurrir a la tipificación de otros delitos⁷⁷⁰ a fin de establecer la construcción de un concepto de terrorismo medianamente completo.

1.2. En relación con la definición de grupo terrorista

La LO 10/1995, de 23 de noviembre, define los grupos terroristas en torno a la finalidad del terrorismo.⁷⁷¹ Conforme al art 571.3:

«[...] se considerarán organizaciones o grupos terroristas aquellas agrupaciones que, reuniendo las características respectivamente establecidas en el párrafo segundo del apartado 1 del artículo 570 bis y en el párrafo segundo del apartado 1 del artículo 570, tengan por finalidad o por objeto subvertir el orden constitucional o alterar gravemente la paz pública mediante la perpetración de cualquiera de los delitos previstos en la Sección siguiente.»⁷⁷²

⁷⁷⁰ Sedición (arts. 544 a 549 LO 10/1995, de 23 de noviembre), atentados contra la autoridad, sus agentes y los funcionarios públicos y resistencia y desobediencia (arts. 550 a 556 LO 10/1995, de 23 de noviembre), maltrato a Fuerza Armada (art. 554 LO 10/1995, de 23 de noviembre), desórdenes públicos (arts. 557 a 561 LO 10/1995, de 23 de noviembre), tenencia, tráfico y depósito de armas, municiones o explosivos (arts. 563 a 570 LO 10/1995, de 23 de noviembre).

⁷⁷¹ Arts. 571 y 572 Ley Orgánica 10/1995, de 23 de noviembre

⁷⁷² Por *Sección siguiente* se refiere a: Sección 2: De los delitos de terrorismo; arts. 572 al 580 de la LO 10/1995, de 23 de noviembre.

Asimismo, expone que los delitos de terrorismo son perpetrados por grupos criminales organizados (art. 570 bis Ley Orgánica 10/1995, de 23 de noviembre), o su en defecto conforme al art. 570 ter, inciso 1, párrafo 2:

«[por] la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas.»

En la Ley Orgánica 2/2015, de 30 de marzo, específicamente en la Sección 1ª ‘De las organizaciones y grupos terroristas’ se mantiene “la misma lógica punitiva”⁷⁷³ que en la regulación previamente descrita, estableciendo la definición de ‘organización o grupo terrorista’ por medio de la normativa anterior, en base a lo enunciado en los art. 570 bis y el art. 570 ter, inciso 1, de la Ley Orgánica 10/1995, de 23 de noviembre.

1.3. En relación con las penas privativas de libertad

El art. 573 bis, de la Ley Orgánica 2/2015, de 30 de marzo, establece

«la pena que corresponde a cada delito de terrorismo partiendo de que si se causa la muerte de una persona se aplicará la pena de prisión por el tiempo máximo previsto en el Código Penal. Esta remisión hace que sea posible, en estos casos, la imposición de la prisión permanente revisable recogida en la reforma del Código Penal operada por LO 1/2015.»⁷⁷⁴

En otro orden de delitos, existe en la Ley Orgánica 2/2015, de 30 de marzo, un incremento de las penas, respecto de la legislación anterior, la Ley Orgánica 10/1995, de 23 de noviembre.

En el caso de los secuestros o detención ilegal, a partir de la modificación de la LO, la pena será de veinte a veinticinco años de prisión si no se tiene razón del paradero de la persona. En el caso de que en el curso de las acciones terroristas se causase aborto o lesiones a una persona la pena será de quince a veinte años de prisión (siendo antes de diez a quince años).

1.4. En relación con la financiación del terrorismo

La Ley Orgánica 10/1995, de 23 de noviembre, en su artículo 576 bis inciso 1 entiende como participación activa del sujeto, quien

“por cualquier medio, directa o indirectamente, provea o recolecte fondos con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte, para cometer cualquiera de los delitos comprendidos en este Capítulo (Capítulo VII: De las organizaciones y grupos terroristas y de los delitos de terrorismo) o para hacerlos llegar a una organización o grupo terroristas”

La principal novedad con relación a la financiación del terrorismo que introduce la Ley Orgánica 2/2015, de 30 de marzo, es la tipificación de las formas imprudentes de la

⁷⁷³ DIARIO LA LEY (2015), opus cit., p. 1.

⁷⁷⁴ *Ibidem*; p. 2

comisión del delito, como “la negligente omisión de los deberes emanados de la normativa sobre blanqueo de capitales y prevención de financiación del terrorismo.”⁷⁷⁵ También se incorpora la responsabilidad penal para las personas jurídicas sobre estos delitos.

2. Los nuevos delitos relacionados con el uso de Internet

Con independencia a los cambios planteados con anterioridad en materia de delitos de terrorismo, que pueden ser analizados comparativamente con la anterior legislación en la materia, la importancia de la Ley Orgánica 2/2015, de 30 de marzo, radica en el hecho de que introduce como nuevo aspecto a considerar en la legislación y a la tipificación punitiva, a Internet contemplando el uso de las nuevas tecnologías de la información como instrumentos de difusión propagandística, para la captación de terroristas y la comisión de delitos.

2.1. Delito de adoctrinamiento y adiestramiento militar o de combate

La Ley Orgánica 2/2015, de 30 de marzo, tipifica mediante el art. 575 el adoctrinamiento y adiestramiento militar o de combate a través de Internet con el objeto de adquirir instrucción en el desarrollo de armas químicas o biológicas, en la elaboración o preparación de aparatos explosivos, inflamables, incendiarios o asfixiantes.

Existe referente a este artículo un elemento de controversia en cuanto se incluye el adoctrinamiento pasivo⁷⁷⁶ en vista de que se castiga con pena de dos a cinco años de prisión quien con la *finalidad de capacitarse para cometer alguno de los delitos tipificados* en el art. 573 de la ley, por medio del acceso a Internet y la utilización de las nuevas tecnologías de la información, revise y/o consulte información de páginas web cuyo contenido esté dirigido o resulte idóneo para incitar a la incorporación de una organización o grupo terrorista; o quien adquiera o tenga en su poder documentos que “estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines.”⁷⁷⁷

El aspecto controversial se presenta en el hecho de que conforme a esta tipificación puede ser penado con pena privativa de libertad quien, por ejemplo, acceda habitualmente a la consulta de páginas web yihadistas o quien tenga almacenado en su ordenador documentos de propaganda terrorista, excluyendo en esta tipificación de delito la consulta por motivos científicos, académicos o meramente informativos.

Adicionalmente se presenta una dificultad en relación con la determinación de la *finalidad de capacitarse para cometer alguno de los delitos tipificados*, en el sentido de

⁷⁷⁵ *Ibidem*.

⁷⁷⁶ En el art. 575.2 de la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁷⁷⁷ *Ibidem*.

que la consulta habitual de páginas web yihadistas no necesariamente conlleva una finalidad última criminal.

2.2. Delito de enaltecimiento o la justificación pública de los delitos de terrorismo

La Ley Orgánica 2/2015, de 30 de marzo, también incorpora modificaciones en el delito de enaltecimiento⁷⁷⁸ del terrorismo en Internet y de incitación a la comisión de actos de terrorismo.

El delito de enaltecimiento, comprendido en el art. 578, enuncia que

«El enaltecimiento o la justificación pública de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución [...] se castigará con la pena de prisión de uno a tres años y multa de doce a dieciocho meses.»

En el caso de que este delito se hubiere cometido a través de tecnologías de la información se acordará adicionalmente la retirada de la red de los contenidos. El mismo artículo indica que:

«Subsidiariamente, [el juez o tribunal] podrá ordenar a los prestadores de servicios de alojamiento que retiren los contenidos ilícitos, a los motores de búsqueda que supriman los enlaces que apunten a ellos y a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos.»

El delito de incitación está recogido en el art. 579 y contempla la difusión de mensajes o consignas para incitar a otros a la comisión de delitos de terrorismo.

«La pena se agrava en el supuesto en que se cometan mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, Internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información, articulando además que los jueces puedan acordar como medida cautelar la retirada de estos contenidos.»⁷⁷⁹

El análisis normativo previo nos introduce sin duda en la tradicional pugna que se libra entre la punición y el respeto de los derechos constitucionales.

En el artículo 2 referente a los ‘Principios fundamentales relativos a la libertad de expresión’, de la Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, se enuncia que, la Decisión Marco no puede bajo ningún aspecto exigir medidas que contradigan los principios fundamentales relativos a la libertad de expresión.

Ello pone de manifiesto la voluntad del Consejo de respetar los derechos y libertades fundamentales en cuanto a libertad de expresión se refiere. Esta declaración resulta necesaria conforme la aplicación de la Decisión Marco 2008/919/JAI representa, en cierta forma, una limitación del uso libre de Internet. Esa restricción no obstante se halla justificada en el ejercicio represivo que las sociedades europeas deben realizar por mandato europeo en beneficio del mantenimiento de la paz y seguridad, nacional e internacional. Extrapolando esta idea a la

⁷⁷⁸ El art. 578 de la Ley Orgánica 10/1995, de 23 de noviembre, no se refiere específicamente a los delitos de enaltecimiento o justificación cometidos a través de Internet.

⁷⁷⁹ DIARIO LA LEY (2015), opus cit., p. 3.

relación que la Unión Europea mantiene con sus EEMM, entendemos que de este modo, los EEMM delegan en una voluntad superior el ejercicio de la autoridad para la pervivencia de la sociedad europea en general.

En el ámbito del Derecho penal resulta ineludible la persecución de conductas de tipo delictivo y la penalización de las mismas. La Decisión Marco 2008/919/JAI del Consejo abre la puerta a la lucha contra los delitos de terrorismo en Internet. Naturalmente resulta primordial y necesario la persecución de todos estos delitos considerando los múltiples avances tecnológicos y los usos con fines criminales que realizan los grupos terroristas de las nuevas tecnologías de la información.

Como se ha descrito previamente, el Derecho de la Unión Europea sirve de base jurídica en la elaboración de las legislaciones internas, dado que estas atienden a las orientaciones de la Unión y a su búsqueda de armonización en el ámbito penal. No obstante, estas orientaciones aun cuando son cada vez más detalladas y específicas en cuanto a la materia sobre la que se debe legislar, no poseen potestad alguna sobre la tipificación de los delitos ni las penas privativas de libertad que debe imponer cada Estado, dado que ello es de competencia exclusiva de cada miembro de la Unión.

Ello hace que exista cierta discrecionalidad por parte de los EEMM, y que se adopten, debido a ello, posturas más o menos restrictivas.

Como ya se ha detallado, en el caso de España, la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal español, adopta las orientaciones de la UE incorporando los nuevos delitos de terrorismo que la Unión ha identificado, pero, con relación a determinados delitos, lo hace con ciertas salvedades que pueden ser interpretadas como vulneraciones constitucionales. Debido a ello, de entre las nuevas tipificaciones que se incorporan a la legislación española, merecen una especial revisión en este sentido el delito de adoctrinamiento pasivo⁷⁸⁰ y el delito de enaltecimiento del terrorismo.

A. Delito de adoctrinamiento pasivo (art. 575.2 LO 2/2015, de 30 de marzo)

El delito de adoctrinamiento pasivo implica que será perseguido bajo esta tipificación quien acceda a un portal de Internet, o quien descargue en su ordenador documentos considerados de adoctrinamiento o adiestramiento terrorista.

Tal como se pronunciaba el presidente de la Audiencia Nacional, José Ramón Navarro Miranda en su ponencia titulada “La Audiencia Nacional y los delitos terroristas: perspectivas actuales y de futuro” en el marco de las VI Jornadas Jurídicas de Ceuta⁷⁸¹, el delito de adoctrinamiento pasivo “permite adelantar la barrera penal.” En este adelanto de la barrera penal, se pueden o deben considerar dos aspectos: 1; desde un punto de vista procesal, obliga a castigar los actos preparatorios del delito; y 2; implica la determinación a

⁷⁸⁰ Recogido en el art. 575.2 de la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁷⁸¹ «España defiende en la UE medidas conjuntas con empresas como Facebook o Twitter para combatir el yihadismo en la red», *Europa Press*, edición online de 3 de julio de 2015. Disponible en: <https://www.europapress.es/nacional/noticia-espana-defiende-ue-medidas-conjuntas-empresas-facebook-twitter-combatir-yihadismo-red-20141009165315.html> [Fecha de consulta: 3 de diciembre de 2023].

priori de una finalidad criminal de las consultas, en detrimento de la libertad de opinión o libertad ideológica.

En relación con el primer punto, la obligación de castigar los actos preparatorios⁷⁸² del delito; es necesario detallar que el Código Penal español establece el principio general de la no punición de los actos preparatorios, salvo aquellos que estén expresamente tipificados, como resulta ser en el caso de la conspiración, provocación y proposición para delinquir. En el caso de la punición de los actos preparatorios no deja lugar a dudas su aplicación en el delito de adoctrinamiento activo⁷⁸³, en cuanto hay una búsqueda manifiesta de establecer una provocación y proposición en otro para delinquir.

La punición de los actos preparatorios del delito de adoctrinamiento pasivo traslada una responsabilidad penal a un sujeto pasivo y hace suponer a priori la comisión de un acto criminal por ser receptor de información.

Referente al segundo punto, la determinación a priori de una finalidad criminal de las consultas es importante mencionar que la propia la Decisión Marco 2008/919/JAI reconoce en cierta forma que las consultas de páginas y sitios de información y propaganda terrorista pueden estar ligados a otra finalidad que no sea criminal al excluir necesariamente estas conductas del ámbito de aplicación de la Decisión Marco.

«La provocación a la comisión de delitos de terrorismo, la captación y el adiestramiento de terroristas son delitos dolosos. Por tanto, nada de lo dispuesto en... [la Decisión Marco 2008/919/JAI] ...podrá interpretarse como un intento de reducir u obstaculizar la difusión de la información con fines científicos, académicos o informativos.»

En adición, en vista de que en el delito de adoctrinamiento pasivo no existe la conspiración, proposición y provocación entre dos o más individuos, sino que se trata de un acto individual de consulta de material terrorista, resulta de suma dificultad determinar la intención de delinquir del individuo. En el camino del delito de adoctrinamiento pasivo nos encontraríamos en la fase interna del delito, es decir la que sucede en la mente del sujeto y que resulta controvertido que sea objeto de materia penal, siendo que *cogitationis poenam nemo patitur*.⁷⁸⁴

B. Delito de enaltecimiento (art. 578 LO 2/2015, de 30 de marzo)

El delito de enaltecimiento, o la justificación pública de los delitos de terrorismo, implica la penalización de actos o expresiones de dichos que glorifiquen o alaben actos terroristas cometidos, o a los autores participantes de su ejecución. Es uno de los nuevos delitos que recibe una nueva tipificación con relación al uso de Internet para su comisión y se encuentra castigado con una pena de prisión comprendida entre uno y tres años.

⁷⁸² Recogidos en arts. 17 y 18 CP, referidos a la conspiración, proposición y provocación para delinquir, en el Derecho penal español, los actos preparatorios son aquellas conductas que realiza el autor de un delito con anterioridad a su ejecución, fase externa del *iter criminis*. Se debe distinguir entre actos preparatorios y tentativa, en virtud de que en la tentativa implica que ya se inició la fase de ejecución del delito. Los actos preparatorios son los que se llevan a cabo en una fase previa al inicio de la ejecución del delito.

⁷⁸³ Recogido en el art. 577.2 de la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁷⁸⁴ ‘*El pensamiento no puede delinquir*’.

En relación con el uso de Internet para la comisión del mismo, cabe señalar que la pena se agrava⁷⁸⁵ siempre que el mensaje se haga público a través de medios de comunicación, Internet o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información.

Teniendo en cuenta que la utilización de medios de comunicación, de Internet, de servicios de comunicaciones electrónicas o de cualquier tipo de tecnología de la información, permite la proyección y difusión del mensaje de forma exponencial, permitiendo que el mismo sea incluso replicado por otros usuarios; este incremento de la pena hace suponer que lo que se persigue es la relación causal, una vez cometido el delito, hacia la capacidad de difusión y proyección del mensaje emitido, es decir, el grado de influencia de la opinión personal.

Resulta controvertido este aspecto en el hecho de que podría estar restringiéndose la libertad de expresión y la libertad de opinión en cuanto, según lo recogido en la propia Decisión Marco 2008/919/JAI,

«la expresión pública de opiniones radicales, polémicas o controvertidas sobre cuestiones políticas sensibles, incluido el terrorismo, queda fuera del ámbito de la presente Decisión Marco y, en especial, de la definición de provocación a la comisión de delitos de terrorismo».

La Decisión Marco 2008/919/JAI busca establecer parámetros de armonización penal en el ámbito europeo con arreglo a los derechos y garantías fundamentales. No obstante, considerando el hecho de que la punición de los delitos de terrorismo queda restringida a la normativa interna, la interpretación puede derivar en legislaciones más o menos restrictivas. En el caso de España y el art. 578 LO 2/2015, de 30 de marzo, referido al delito de enaltecimiento, se hace referencia en el inciso 3 la necesidad de un incremento de las penas en su mitad superior cuando “los hechos a la vista de las circunstancias resulten idóneos para alterar gravemente la paz pública o crear un grave sentimiento de inseguridad en la sociedad.”

Para varios autores, esta forma de entender el Derecho penal es controvertida. Según Carmen Martínez Perza, el traslado de esta percepción basada en los sentimientos de inseguridad de la sociedad pone de manifiesto la intención de sostener un populismo punitivo acrecentado por la propaganda gubernamental de alarma hacia la población por medio de los medios de comunicación.⁷⁸⁶

En este mismo sentido, Díez Ripollés establece su propia crítica al populismo punitivo al referirse al miedo al delito, como un estado de opinión que se encuentra presente en los discursos en torno al fenómeno del terrorismo, “propiciando una respuesta punitiva exagerada e incoherente”⁷⁸⁷

⁷⁸⁵ Art 578.2: “Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, Internet o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información.”

⁷⁸⁶ MARTÍNEZ PERZA, Carmen. «La reforma del Código Penal de 2010», *Derecho Penitenciario*, artículo de opinión, pp. 18-26. Disponible en: <http://www.derechopenitenciario.com/comun/fichero.asp?id=2160> [Fecha de consulta: 3 de diciembre de 2023].

⁷⁸⁷ Díez RIPOLLES, José Luis (2005): «De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado», *Revista Electrónica de Ciencia Penal y Criminología*, N.º 7, p. 14.

Con independencia de esta legislación puntual, resulta determinante el hecho de que ya en 1999, Silva Sánchez empleaba la expresión ‘expansión del Derecho penal’ en referencia a determinados rasgos que consideraba definitorios del Derecho penal español del momento, indicando que no resultaba tarea difícil la observación de una

«[...] tendencia claramente dominante en la legislación de todos los países hacia la introducción de nuevos tipos penales, así como a una agravación de los ya existentes que cabe enlazar en el marco general de la restricción, o la ‘reinterpretación’ de las garantías clásicas del Derecho penal sustantivo y del Derecho procesal penal. Creación de nuevos ‘bienes jurídico-penales’, ampliación de los espacios de riesgos jurídico-penalmente relevantes, flexibilización de las reglas de imputación y relativización de los principios político-criminales de garantía, no serían sino aspectos de esta tendencia general, a la que cabe referirse con el término de ‘expansión’.»⁷⁸⁸

Ello da cuenta de que la tendencia del Derecho penal español a ser expansivo no es algo que surja a necesidad de la Unión Europea, sino que se observa una tradición en este ámbito. Conforme a Felip I Saborit esta tendencia perdura en la actualidad, evidenciando una “huida” hacia el Derecho penal en la búsqueda de resolver “los grandes problemas sociales”. Asimismo, divide la expansión del Derecho penal en dos vertientes, la extensiva y la intensiva. La primera se caracterizaría por aplicarlo a entornos hasta el momento ajenos a su intervención; mientras que la segunda, consistiría en la profundización del Derecho penal en ámbitos en los que su penetración era ya incipiente, como es el caso del terrorismo.⁷⁸⁹

En el ámbito del terrorismo es común referirse a la lucha armada. Para López Peregrín esto establece una diferencia entre dos clases de delincuentes. Esta diferencia se pone de manifiesto por medio de diversas excepciones al régimen general del Código Penal y se aplica sobre los delitos de terrorismo y para los cometidos en el seno de organizaciones criminales. Según López Peregrín, esto representa una vulneración del principio de igualdad al tratar a los delincuentes no como ciudadanos, sino como enemigos.⁷⁹⁰ En palabras de Cancio Meliá, “como meras fuentes de peligro que deben ser neutralizadas del modo que sea, cueste lo que cueste.”⁷⁹¹

En el caso de los delitos cometidos a través de Internet, para Puente Guerrero, el problema principal está dado en el hecho de que las nuevas estrategias de seguridad se materializan en un ejercicio de control extremo sobre los riesgos, en la búsqueda de prevenir la comisión de nuevos delitos. Por lo tanto, estas medidas “persiguen una finalidad incapacitante y suelen consistir en la restricción de movimientos, mediante la vigilancia electrónica.”⁷⁹²

⁷⁸⁸ SILVA SÁNCHEZ, Jesús María (2001): *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, Madrid: Civitas, p. 20.

⁷⁸⁹ FELIP I SABORIT, David. (2010): «Observaciones a La Expansión diez años después», en: ROBLES PLANAS, Ricardo y SÁNCHEZ-ORTIZ GUTIERREZ, Pablo (Coords.), *La crisis del Derecho penal contemporáneo*, vol. 21, Barcelona, Atelier, p. 64.

⁷⁹⁰ LÓPEZ PEREGRÍN, Carmen. (2003): «¿Lucha contra la criminalidad mediante el cumplimiento íntegro y efectivo de las penas?», *Revista Española de Investigación Criminológica*, N.º 1, p. 8.

⁷⁹¹ CANCIO MELIÁ, Manuel (2009): «Sentido y límites de los delitos de terrorismo en Derecho penal Contemporáneo», *Revista Internacional*, N.º 26, p. 52-54.

⁷⁹² PUENTE GUERRERO, Patricia (2011): «La regulación de los delitos de terrorismo en la L.O. 5/2010. ¿Son los terroristas nuestros “enemigos”? Especial referencia a la libertad vigilada», *Derecho penal y Criminología*, Vol. 32, No. 93, julio-diciembre, p. 104

Esta vigilancia, sumada a la concepción criminológica del fenómeno del terrorismo puede establecer la noción de que el recorte de garantías otorgadas por el Estado de Derecho pueda estar justificado en la consecución de los fines propios de la persecución de los crímenes de terrorismo, actuando en ocasiones sin proporcionalidad y/o denotando como terrorismo, específicamente en la tipificación de adoctrinamiento pasivo y enaltecimiento, acciones u opiniones que no necesariamente representan finalidad criminal.

MEDIDAS DE CONTROL Y VIGILANCIA, Y REPRESIÓN CONTRA EL YIHADISMO EN INTERNET

España es un Estado con una gran andadura en el ámbito de la lucha contra el terrorismo. Su experiencia con el terrorismo nacionalista de ETA le otorgó a este Estado un período histórico que, aunque trágico, ha sabido capitalizar en términos institucionales para el desarrollo de políticas públicas que le permitieran hacer frente a este fenómeno.

Así, por ejemplo, entre las primeras medidas de carácter operativo adoptadas se encuentra la creación en el año 1977 del Grupo Especial de Operaciones (G.E.O.). El Grupo G.E.O.⁷⁹³ es una unidad del Cuerpo Nacional de Policía (C.N.P.) cuyos miembros son entrenados para intervenir y resolver situaciones especialmente críticas. El Grupo G.E.O. está inspirado en el grupo antiterrorista alemán GSG-9 y su finalidad específica en España es luchar contra el terrorismo nacional e internacional y contra los diversos grupos de delincuencia organizada. La organización de este grupo comando se compone por una sección operativa que es aquella sobre la que recae el cumplimiento de misiones específicas y también por una sección de apoyo que facilita que la sección operativa pueda realizar su cometido con éxito. Si bien el Grupo G.E.O. ha nacido para dar respuesta a las acciones delictivas que tenían lugar en España en la década de 1970, el grupo se ha adaptado de forma paulatina conforme las modalidades del crimen de terrorismo y delincuencia organizada se modificaban. En el ámbito del terrorismo, el delito evolucionó desde un terrorismo nacional de ETA, hacia un terrorismo internacional, y posteriormente hacia el terrorismo yihadista global. En el ámbito de la delincuencia organizada, la creciente internacionalización de las organizaciones criminales ha supuesto que el Grupo G.E.O. intervenga en operaciones conjuntas y coordinadas debido a que las acciones criminales de los actuales organizaciones son fundamentalmente transnacionales y transfronterizas.

Sí bien todo el Cuerpo Nacional de Policía de España se encuentra involucrado en las acciones de contraterrorismo, la adaptación del Grupo G.E.O. al nuevo terrorismo yihadista global ha sido significativa porque ha supuesto un reaprendizaje en todo sentido. Aprender sobre cuáles son grupos terroristas, cuáles son sus métodos de acción delictiva, cómo se identifica al sujeto delictivo, etc. Todo ello ha llevado a la implementación de programas específicos para el Grupo G.E.O. como la denominada Operación Madrid. La operación Madrid es un dispositivo puesto en marcha en el año 2017 por el Ministerio del Interior a fin de garantizar que el Grupo de Operaciones Especiales (G.E.O.) sea capaz de reaccionar ante un posible atentado en Madrid en solo cuestión de minutos. Ello establece que “efectivos de esa unidad de élite patrullan de forma constante por las calles del centro de la capital para rebajar al mínimo el tiempo de intervención

⁷⁹³ Conocido coloquialmente en la sociedad española como ‘los GEOS.’

ante un hipotético ataque”⁷⁹⁴ con la orden de tirar a matar a viandantes y a conductores peligrosos e identificados como presuntos terroristas. Esta medida, juntamente con las medidas de protección física de espacios públicos⁷⁹⁵, posee su fundamento en las acciones criminales ejecutadas por el terrorismo en Europa (Paris y Berlín) y en España (atentados del 17-A) en los años inmediatos previos a esta implementación del Ministerio del Interior.⁷⁹⁶ La premisa del Ministerio es que el tiempo de ejecución del que dispone el terrorista agrava el atentado. Los ejemplos citados comparten este criterio. En el atentado de Paris, debido a la toma de rehenes, los yihadistas dispusieron de un total de 2 horas y 38 minutos para llevar a cabo todo tipo de acción criminal que implicó incluso actos de tortura y mutilación.

La implementación de la Operación Madrid en la que el Grupo G.E.O. es capaz de intervenir en minutos para impedir o detener el desarrollo de un atentado terrorista es una muestra de que, en el ámbito institucional y operativo tendiente a la represión del crimen de terrorismo, España posee un alto nivel preventivo caracterizado por una gran cultura del control. La tendencia de su Política Criminal actual se orienta en el delito de terrorismo yihadista al *warfare*⁷⁹⁷, es decir, a tratar al terrorista como en un escenario de guerra.

No obstante, este modelo no se establece con esta implementación ministerial sobre la Policía Nacional y los Grupos G.E.O., sino antes. En términos generales España, posee una orientación de su Política Criminal de carácter anticipatorio que le ha llevado a la adopción de medidas de similar característica de forma previa.

Por ejemplo, en el orden de las medidas institucionales de lucha contra el terrorismo desarrolladas por el Estado, es menester mencionar la aprobación, en enero de 2015, del Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV).⁷⁹⁸ Se trata de un instrumento, coordinado desde el Ministerio del Interior, que busca prevenir y evitar el surgimiento y desarrollo de procesos de radicalización terrorista.

⁷⁹⁴ «Un comando de geos patrulla de incógnito las calles de Madrid para abatir yihadistas», *El Confidencial*, edición online de 29 de agosto de 2017. Disponible en: https://www.elconfidencial.com/espana/2017-08-28/geo-abatir-patrulla-operacion-madrid_1434118/ [Fecha de consulta: 21 de septiembre de 2022].

⁷⁹⁵ Se refiere a la colocación de grandes maceteros o bolardos para tratar de reducir el riesgo de atropello masivo en fechas navideñas o en lugares públicos en donde exista una alta concentración personas.

⁷⁹⁶ Paris (13 de noviembre de 2015): Atentado yihadista en el teatro de variedades Bataclan, seis bares y restaurantes y el perímetro del estadio deportivo Stade de France. En el atentado fallecieron 130 personas y se contabilizaron más de 400 heridos. Berlín (19 de diciembre de 2016): Atentado yihadista en un mercado navideño en Breitscheidplatz, Charlottenburg. Un terrorista embistió con un camión a una multitud de personas. En el atentado fallecieron 11 personas, y 56 personas resultaron heridas. Barcelona (17 de agosto de 2017): Atentado yihadista en Las Ramblas, Barcelona. Un terrorista embistió con una furgoneta a personas que paseaban por La Rambla. El conductor recorrió más de 500 metros atropellando personas. En el atentado fallecieron 15 personas y 131 resultaron heridas. Cambrils (17 de agosto de 2017): Atentado yihadista en un control policial de los Mozos de Escuadra. Atropello y fallecimiento de 6 personas. Estos dos últimos atentados son conocidos en España como los atentados del 17-A. Investigaciones posteriores realizadas por los Mozos de Escuadra indicaron que el 17 de agosto de 2017 estaba previsto también atacar Barcelona y París simultáneamente, colocando ‘furgonetas bomba’ en la Sagrada Familia y la Torre Eiffel. De haber prosperado estos ataques podrían haber sido los mayores atentados terroristas en la historia de Europa

⁷⁹⁷ *Warfare* es un término acuñado en 1980. Hace referencia a una de las tendencias que puede adoptar la Política Criminal de un Estado aún en tiempos paz. El *warfare*, como antítesis al *welfare* que se caracteriza por la promoción del Estado de bienestar moderno y que promueve una Política Criminal de índole social, consiste básicamente en tratar policial, jurídica y penitenciarmente al delincuente como si se estuviera en guerra. El *warfare* se centra en la víctima y en cómo protegerla, se centra en la prevención del delito de forma proactiva y anticipada, otorga importancia a la opinión pública, y es un modelo en donde prima la seguridad ciudadana y pública.

⁷⁹⁸ MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA (2015): *opus cit.*

Este Plan Estratégico posee un enfoque multidisciplinar y distingue tres ámbitos y tres áreas de actuación. En cuanto a los ámbitos, el Plan se desarrolla en el ámbito interno (España), el ámbito externo (fuera de España) y el ciberespacio (Internet). Ello establece ‘dónde’ deben realizarse las acciones del Estado. En cuanto a las tres áreas, el Plan se desarrolla en la prevención (antes del hecho), vigilancia (durante el hecho) y actuación (después del hecho). Ello indica ‘cómo’ y ‘cuándo’ tienen que llevarse a efecto las acciones anteriormente previstas.

En el caso puntual del ámbito del ciberespacio, el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta prevé un tratamiento de la red a través de fuentes abiertas, es decir, la estructura de vigilancia⁷⁹⁹ prevista conocerá de la información que circule libremente por la red que pueda ser considerada fuente de radicalización. De forma específica en este ámbito, una Unidad de Tratamiento de la Red, ubicada en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) analizará la información obtenida por este medio.

El Plan Estratégico Nacional de Lucha contra la Radicalización Violenta fue elaborado⁸⁰⁰ en la búsqueda del cumplimiento de las Directrices de la Unión Europea de lucha contra la radicalización y el extremismo violento, descritas en la “Estrategia de la Unión Europea de Lucha contra el Terrorismo”⁸⁰¹ adoptada por el Consejo en el año 2005, y la “Estrategia contra la Radicalización y la Captación de Terroristas” del año 2014.

Si bien el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta ha sido adoptado el 30 de enero de 2015, España ya había planteado un año antes la necesidad de vigilar Internet y había defendido su posición al respecto frente a la Unión Europea planteando esta necesidad de mayores medidas de colaboración entre los Estados Miembros con compañías privadas como *Facebook* o *X* (ex *Twitter*), a fin de aunar esfuerzos para combatir el terrorismo yihadista en la red.⁸⁰²

Concretamente, el 9 de octubre de 2014, en el marco de una reunión del Consejo de Ministros de Justicia y Asuntos de Interior de la Unión Europea (JAI) celebrada en Luxemburgo, entre sectores públicos⁸⁰³ y privados,⁸⁰⁴ el secretario de Estado de Seguridad de España, Francisco Martínez, aseguro que,

«[...] el uso de Internet es un elemento común en la mayoría de las operaciones que se han llevado a cabo en España contra el terrorismo yihadista y que, por ello, es necesario trabajar en estrecha colaboración para hacer de la colaboración público-privada la herramienta clave en la lucha contra este fenómeno y que, a su vez, permita imponer una contra narrativa que anule los mensajes de los radicales en la red.»⁸⁰⁵

⁷⁹⁹ Integrada por Doce ministerios, el CNI, la Federación Española de Municipios y Provincias (FEMP), la Fundación Pluralismo y Convivencia y otras entidades públicas o privadas que se consideren necesarias (por ej. universidades, asociaciones, ONGD, etc.).

⁸⁰⁰ Elaborado bajo la coordinación del actual Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (ex Centro Nacional de Coordinación Antiterrorista), por un grupo compuesto por doce ministerios, el CNI, la Fundación Pluralismo y Convivencia y la Federación Española de Municipios y Provincias (FEMP).

⁸⁰¹ Primera Estrategia desarrollada por la Unión Europea, orientada a las acciones institucionales de contraterrorismo.

⁸⁰² «Francisco Martínez afirma en Luxemburgo ante la industria de Internet que la ‘colaboración público-privada es una herramienta clave en la lucha contra el yihadismo’ en la Red», *La Moncloa*, 9 de octubre de 2014. Disponible en: <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2014/101014jailuxemburgo.aspx> [Fecha de consulta: 21 de septiembre de 2022].

⁸⁰³ Entre ellos, la Comisaria de Asuntos de Interior en la Comisión Europea y la presidencia italiana del Consejo Europeo.

⁸⁰⁴ Entre otros, directivos de las empresas proveedoras de servicios de Internet, como *Microsoft*, *Google*, *Facebook* y *X* (ex *Twitter*).

⁸⁰⁵ «España defiende en la UE medidas conjuntas con empresas como Facebook o Twitter para combatir el yihadismo en la red», *Ibidem*.

En el marco de esta reunión, Francisco Martínez instó a los otros EEMM y a los máximos responsables de las empresas de tecnología en Internet a desarrollar medidas para fomentar la colaboración entre el sector público y privado.

Entre las medidas propuestas estipuló la necesidad de crear herramientas tecnológicas que faciliten el trabajo de los investigadores como programas de geolocalización o softwares de navegación encubierta. Uno de los elementos más significativos de esta intervención fue la propuesta que realizó España de que se cree o designe un punto de contacto institucional estable y permanente entre ambos sectores, el público y el privado, es decir entre la Unión Europea y sus EEMM con las empresas de tecnología en Internet. Esta aportación es particularmente relevante habida cuenta de la creación de EU IRU dentro de Europol, exactamente al año siguiente.

Es precisamente en esta reunión en la que España insistió en la necesidad de trabajar conjuntamente y de impulsar la realización conjunta de actividades formativas, en donde se anunció la presentación del Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV) que implementaría el Estado español.

En consonancia con la persecución de los delitos de terrorismo en Internet, el 1 de junio de 2015, el presidente de la Audiencia Nacional, José Ramón Navarro Miranda, expresó en el marco de las VI Jornadas Jurídicas de Ceuta organizadas por el Gobierno autonómico, el Consejo General del Poder Judicial (CGPJ) y el Centro universitario local de la UNED, que Internet es “sin duda, el gran arma terrorista del yihadismo”, destacando que dicha amenaza debe de combatirse “por la vía de la cooperación internacional”. Asimismo, consideró que la reforma del Código Penal⁸⁰⁶ “permite adelantar la barrera penal frente al adoctrinamiento pasivo, ante aquellas personas que entren en Internet en búsqueda de esas páginas yihadistas, o frente a quienes viajan al extranjero para practicar la supuesta yihad.”⁸⁰⁷

Actualmente, las Fuerzas y Cuerpos de Seguridad del Estado español cuentan con unidades especializadas que les permiten monitorizar la red y detectar contenidos radicales o con fines terroristas a fin de implementar su Política Criminal en esta materia.

Dentro del Cuerpo Nacional de Policía (C.N.P.) se encuentra la Comisaría General de Información⁸⁰⁸ (CGI) dependiente de la Dirección Adjunta Operativa. Las funciones de la Comisaría General de Información⁸⁰⁹ se centran en la captación, recepción, tratamiento y desarrollo de toda la información de interés para asegurar el orden y la seguridad ciudadana. Asumen, además, de forma operativa la información acerca de los delitos de terrorismo cometidos en el ámbito nacional e internacional. Dentro de su estructura se encuentran los Técnicos Especialistas en Desactivación de Artefactos Explosivos (TEDAX-NRBQ). La organización interna de la Comisaría General de Información es secreta, solo se ha dado a

⁸⁰⁶ En referencia a la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

⁸⁰⁷ *Ibidem*.

⁸⁰⁸ La Comisaría General de Información obtuvo en los Acuerdos del Consejo de Ministros del 28.11.1986 y 16.02.1996, “el carácter de secreto a su estructura, organización, medios y procedimientos operativos específicos utilizados a fin de desarrollar los servicios de información.” Véase: Comisaría General de Información, *Policía Nacional*. Disponible en: <https://www.policia.es/es/tupolicia/conocenos/estructura/dao/cginformacion.php> [Fecha de consulta: 22 de noviembre de 2023].

⁸⁰⁹ Durante el régimen franquista, esta unidad se denominó Servicio de Información y Jefatura de Información, y coloquialmente fue conocida como policía secreta por los medios de comunicación, y la sociedad española.

conocer que se divide en cinco unidades operativas,⁸¹⁰ las cuales han sido modificadas tras los atentados del 11-M.

Las cinco unidades operativas actuales son 1) la Unidad Central de Inteligencia (UCI) que asume las funciones de análisis en materia de inteligencia. Está conformada por dos brigadas: la Brigada de Análisis Estratégico y Operativo de la Información (que se especializa en el análisis y tratamiento de la información sobre terrorismo yihadista) y La Brigada de Sistemas y Tecnologías de la Información y Ciberterrorismo; 2) la Unidad Central de Información Interior (UCIO) que asume la investigación acerca de movimientos extremistas y subversivos, crimen organizado, sectas y organizaciones que puedan suponer una potencial o real amenaza a la seguridad; 3) la Unidad Central de Información Exterior (UCIE) que se orienta a la obtención de información procedente del exterior, al intercambio de información con servicios extranjeros, y a la prevención, seguimiento, control y neutralización de las actividades de los grupos terroristas y radicales violentos en España y Estados socios; 4) la Unidad Central Operativa Antiterrorista (UCOA) que realiza las labores operativas en materia antiterrorista como acciones de seguimiento, operaciones, infiltraciones, etc.; y, 5) la Unidad de Apoyo Operativo (UAO) que se encarga de garantizar el apoyo logístico al resto de unidades.

El Cuerpo Nacional de Policía (C.N.P.) también posee la Comisaría General de Policía Judicial (C.G.P.J.), y ésta, a su vez, posee diversas unidades que trabajan de forma especializada, mediante metodologías de investigación criminal y actividades operativas. Las unidades que posee son⁸¹¹: Unidad Central de Droga y Crimen Organizado (realiza la investigación y persecución, en los ámbitos nacional y transnacional, de toda actividad delictiva relacionada con el tráfico de drogas), Unidad Central de Delincuencia Especializada y Violenta (que agrupa la Brigada Central de Investigación de la Delincuencia Especializada, la Brigada Central de Investigación de Delitos contra las Personas, y la Brigada del Patrimonio histórico), la Unidad Central de Inteligencia Criminal (posee funciones de desarrollo y seguimiento y control de planes estratégicos y operativos en inteligencia y planificación), la Unidad Central de Delincuencia Económica y Fiscal (que engloba la Brigada Central de Delincuencia Económica y Fiscal, la Brigada Central de Investigación de Blanqueo de Capitales y Anticorrupción, la Brigada Central de Inteligencia Financiera, la Brigada de Investigación del Banco de España, y la Unidad Adscrita a la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada), y la Unidad de Investigación Tecnológica (Asume la investigación y persecución de las actividades delictivas que impliquen la utilización de nuevas tecnologías).

Es precisamente la Unidad de Investigación Tecnológica (U.I.T.) de la Policía Nacional la que se encarga de todos los ciberdelitos que tienen lugar en el ámbito nacional y transnacional, entre ellos, los delitos de terrorismo. Funge además como Centro de Prevención y Respuesta E-Crime de la Policía Nacional. Dentro de la U.I.T. se encuentra la Brigada Central de Investigación Tecnológica (B.C.I.T.), cuyo cumplimiento de funciones se encuadra en responder a los retos que plantean las nuevas formas de delincuencia por medio del uso de Internet. La B.C.I.T. asume competencia directa en las investigaciones llevadas a cabo dentro de la Unión Europea, iniciadas por Europol o por otros EEMM, en donde los delitos de terrorismo sean cometidos por medio del uso de Internet. Además, coordina operaciones en donde se encuentren involucradas otras

⁸¹⁰ Unidad Central de Inteligencia UCI, *Intelpage*. Disponible en: <https://intelpage.info/unidad-central-de-inteligencia-uci.html> [Fecha de consulta: 22 de noviembre de 2023].

⁸¹¹ Comisaría General de Policía Judicial, *Policía Nacional*. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php [Fecha de consulta: 22 de noviembre de 2023].

Jefaturas Superiores del C.N.P., e interviene en la formación del personal de la Policía Nacional en esta materia y de otros cuerpos policiales extranjeros.⁸¹²

Además de la Brigada Central de Investigación Tecnológica (B.C.I.T.) del C.N.P., España cuenta con el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil, otra unidad fundamental orientada a la persecución de los delitos terroristas mediante el uso de Internet.

El Grupo de Delitos Telemáticos (GDT) fue creado en el año 1996,⁸¹³ para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet. Posee una estructura organizada en Equipos de Investigación Tecnológica (EDITE,s). Los EDITE,s están presentes en cada una de las provincias de España, y se encargan coordinadamente, con el Grupo de Delitos Telemáticos de la:

«[...] investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión y participan activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Grupo de Europol.»⁸¹⁴

Para combatir el terrorismo y otras formas de delincuencia grave transnacional en Internet, España se apoya en unidades de especial operación y desarrollo en Internet, y en diversas estrategias que determinan el desarrollo del trabajo por realizar en esta materia.

El 21 de enero de 2019, España aprueba la *Estrategia Nacional Contra el Terrorismo*⁸¹⁵ llevada adelante por el Ministerio del Interior y el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). La estrategia, que cuenta con la colaboración de Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, el Ministerio de Justicia, el Ministerio de Defensa y el Departamento de Seguridad Nacional, se estructura en torno a cuatro pilares: Prevenir, Proteger, Perseguir y Preparar la respuesta.⁸¹⁶ Esta Estrategia Nacional recuerda indudablemente a la *Estrategia de la Unión Europea de Lucha contra el Terrorismo* del año 2005, cuyos cuatro pilares eran Prevenir, Proteger, Perseguir y Responder. Es indiscutible que la Estrategia Nacional de España responde a los intereses de la Unión sobre estas cuatro vertientes (Prevenir, Proteger, Perseguir y Responder) que abarcan completamente todo el abanico de la Política Criminal en cuanto al terrorismo se refiere. No obstante, no deja de resultar llamativo el hecho de que la elaboración, en España, de un documento de semejante importancia sea desarrollado más de diez años después de que la orientación política fuera dada por Europa. Los ejes ‘Proteger’, ‘Perseguir’ y ‘Preparar la Respuesta’ de la Estrategia Nacional Contra el Terrorismo de 2019 se centran en velar por la seguridad de los ciudadanos, instituciones e intereses nacionales frente al terrorismo y frente a cualquier forma de extremismo violento. También de orientar las estrategias de acción operativa para investigar y detener autores y

⁸¹² «Los 'ciberpolicías' de España: así es la Brigada Central de Investigación Tecnológica», *Periódico 20 minutos*, edición online de 20 de enero de 2023. Disponible en: <https://www.20minutos.es/tecnologia/ciberseguridad/quien-es-y-como-actua-la-policia-cibernetica-en-espana-5093449/> [Fecha de consulta: 23 de noviembre de 2023].

⁸¹³ En 1996 tenía el nombre de Grupo de Delitos Informáticos (GDI), tiempo después se denominó Departamento de Delitos de Alta Tecnología (DDAT), y finalmente Grupo de Delitos Telemáticos (GDT). Véase: «GDT Grupo de Delitos Informáticos», *Guardia Civil*. Disponible en: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php [Fecha de consulta: 22 de noviembre de 2023].

⁸¹⁴ *Ibidem*.

⁸¹⁵ Orden PCI/179/2019, de 22 de febrero, por la que se publica la Estrategia Nacional contra el Terrorismo 2019, aprobado por el Consejo de Seguridad Nacional.

⁸¹⁶ «El Gobierno hace pública por primera vez la Estrategia Nacional contra el Terrorismo», *La Moncloa*, 26 de febrero de 2019. Disponible en: <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2019/260219-estrategia.aspx> [Fecha de consulta: 23 de noviembre de 2023].

ponerlos a disposición judicial, así como buscar la reparación del daño causado mediante la asistencia a víctimas y la restauración de la normalidad social. Estos tres ejes hacen referencia a la necesidad de legislación y de instituciones dentro de un Estado que permitan la persecución y la represión del crimen.

Dentro de la Estrategia señalada existe un primer eje, que hemos dejado para el final denominado ‘Prevenir’. Este eje se encarga del desarrollo de estrategias orientadas a impedir el desarrollo y la expansión del terrorismo en España, y lo veremos a continuación.

MEDIDAS PREVENTIVAS Y CAMPAÑAS DE INFORMACIÓN

La *Estrategia Nacional Contra el Terrorismo*⁸¹⁷ desarrollada en España, en el año 2019, por el Ministerio del Interior y el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) establece dentro de su primer eje la necesidad del prevenir el terrorismo.

Esta Estrategia se ha elaborado teniendo en cuenta las orientaciones que ha propuesto oportunamente la Unión Europea para desarrollar modelos preventivos dentro de la Política Criminal de cada Estado Miembro. Estos modelos preventivos que la UE ha propuesto ya han sido implementados dentro de la Unión, en algunos casos mediante la difusión de una contranarrativa terrorista, y en otros casos mediante un aparato mecanicista que ha logrado establecer trabas a los usos de Internet por parte del yihadismo que ha desalentado la comisión de cualquier tipo de acto terrorista.

Como ha sucedido antes con el Derecho penal y con el sistema institucional que permite luchar contra el terrorismo, las acciones preventivas desarrolladas por la UE han servido de referencia y modelo para la creación de medidas nacionales basadas en esta vertiente cautelar. No obstante, las orientaciones de la Unión son seguidas con cierto grado de discrecionalidad por parte de cada uno de los Estados Miembros, de forma tal que cada Estado adopta las recomendaciones y las orientaciones de la Unión, pero les da forma en el ámbito interno conforme a su propia Política Criminal. Así, por ejemplo, en el caso de España se observa que las medidas de prevención contra el terrorismo yihadista en Internet han ocupado, dentro de su Política Criminal, el último peldaño de importancia.

En la última estrategia adoptada en el año 2019, *Estrategia Nacional Contra el Terrorismo*, se encuentra un capítulo denominado “Prevenir: Actuar contra las causas”, cuyos ejes prioritarios son los siguientes:

- Revisar, actualizar y desarrollar el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV).
- Impulsar y reforzar la coordinación y colaboración de todos los organismos e instituciones, tanto públicas como privadas, en la lucha contra los extremismos violentos, promoviendo la participación ciudadana en el ejercicio de la responsabilidad colectiva.
- Adecuar de manera continuada la acción legislativa del Estado a la evolución del fenómeno del terrorismo y el extremismo violento, proporcionando un tratamiento preventivo que incorpore las dimensiones de género y de edad.

⁸¹⁷ ESTRATEGIA NACIONAL CONTRA EL TERRORISMO (2019): Ministerio del Interior y Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). Aprobado por el Consejo de Seguridad Nacional según orden PCI/179/2019, de 22 de febrero.

- Reforzar las medidas para la prevención de la financiación del terrorismo y los extremismos violentos.
- Impulsar una comunicación estratégica eficaz y proactiva frente al mensaje radical sobre la base de los valores democráticos reconocidos en la Constitución, favoreciendo la implicación de todos los actores y de la sociedad en su conjunto.⁸¹⁸

La Estrategia enuncia a su vez que estos ejes prioritarios se aplicarán en lo que se reconoce como “ámbito interno” (dentro de España), “ámbito externo” (en un contexto de colaboraciones con la UE, ONU, OTAN, Consejo de Europa, y otras iniciativas internacionales), y “ámbito de los espacios comunes globales” (referido puntualmente al ciberespacio). En una búsqueda de una mayor especificidad, dentro del “ámbito de los espacios comunes globales”, encontramos a su vez la existencia de nueve líneas estratégicas, en las que España trabajará preventivamente para evitar la comisión de acciones terroristas en Internet. Estas nueve líneas estratégicas son:

1. Promover iniciativas a nivel nacional e internacional, especialmente en el seno de la Unión Europea que aúnen esfuerzos, incluyendo una legislación homogénea que permita la máxima eficacia en este ámbito.
2. Impedir el alojamiento de contenidos y canales que promuevan el adoctrinamiento, reclutamiento, y difusión de propaganda relativa a terrorismo o movimientos extremistas violentos.
3. Fomentar y coordinar las relaciones público-privadas en este ámbito, con el objetivo de producir sinergias eficaces que dificulten el uso del ciberespacio con fines terroristas o extremistas de carácter violento.
4. Generar una narrativa propia y específicamente dirigida a los colectivos vulnerables contra los procesos de radicalización violenta.
5. Promover campañas en Internet y redes sociales que hagan frente al discurso extremista violento, colaborando e implicando especialmente a la sociedad civil y al colectivo de los jóvenes.
6. Fomentar una comunicación eficaz, que permita transmitir la posición y actividad del Estado en relación con el terrorismo y el extremismo violento, así como sensibilizar del peligro que conlleva, con el especial apoyo y colaboración de los diferentes medios de comunicación y actores involucrados.
7. Conocer y actuar sobre las vulnerabilidades de los nuevos canales de movimientos de bienes y fondos activos virtuales que surgen como consecuencia de las innovaciones tecnológicas.
8. Fomentar la información y conocimiento de los espacios comunes globales, su vulnerabilidad y su posible uso con fines terroristas o de violencia extremista.
9. Potenciar el conocimiento y la utilización de canales directos, en tiempo real, de relación entre el ciudadano y la Administración para la comunicación y alerta de situaciones de riesgo, incluidos entre otros, el Centro de Coordinación de Información sobre la Radicalización (CCIR) y los habilitados por los organismos de seguridad e inteligencia.⁸¹⁹

Dentro de cada una de las líneas estratégicas acordadas, encontramos el enfoque preventivo de Peter Lejins, concretamente en el “ámbito de los espacios comunes globales”, encontramos orientaciones preventivas mecánicas (concretamente los puntos 2, 3, 7 y 9), ello quiere decir, establecer medidas que tratan de crear obstáculos para la comisión del delito y que buscan un “cerrar” el camino del delincuente. También, dentro de esta línea estratégica encontramos las medidas de prevención punitiva (punto 1), estas son todas aquellas que se fundamentan por medio de la amenaza penal, y finalmente encontramos las medidas de prevención correctiva (en esta línea estratégica son los puntos 4, 5, 6 y 8), que se caracterizan por detectar y eliminar, o reducir sustancialmente, los factores criminógenos⁸²⁰ en la vida de los grupos y sujetos en riesgo

⁸¹⁸ *Ibidem*, pág. 36.

⁸¹⁹ *Ibidem*, pág. 42

⁸²⁰ Elementos que aunados entre sí contribuyen a un determinado resultado criminal.

de resultar potenciales autores de delitos terroristas, es decir, eliminar las causas potenciales para evitar que la conducta delictiva tenga lugar.⁸²¹

En retrospectiva, entre las directrices del Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV) implementado en el año 2015 ya se expresaba la intención manifiesta de imponer una contranarrativa que permita minimizar los efectos del enaltecimiento.⁸²² La Estrategia de ese entonces, al igual que la Estrategia Nacional Contra el Terrorismo de 2019, también se desarrollaba en tres ámbitos (“interno”, “externo” y “ciberespacio”) y preveía tres áreas de actuación (“prevenir”, “vigilar” y “actuar”) por cada uno de los ámbitos señalados. Es precisamente en el área de “prevenir” en todos sus ámbitos de aplicación (“interno”, “externo” y “ciberespacio”) en donde no existe casi desarrollo de contenido. Es decir, preventivamente con respecto al terrorismo yihadista en Internet, España no realizaba propuesta alguna y realizaba todas las acciones de lucha contra el terrorismo mediante instrumentos jurídicos punitivos y mediante actuaciones de ejecución operativa. Debido a ello, el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV) del año 2015, sí bien es un documento rector en España en la lucha contra el terrorismo yihadista en Internet, centra toda su atención en los incisos denominados “vigilar” y “actuar”, cuyo contenido se orienta al reforzamiento del Derecho penal y al reforzamiento de la estructura institucional. Dentro de esta estrategia, incluso en el escaso desarrollo del área de la prevención dicho reforzamiento de la estructura institucional había adquirido implicaciones punitivas, dado que el propio PEN-LCRV detalla que:

«[...] A nivel institucional el Ministerio del Interior, bajo el nombre de Stop Radicalismos⁸²³, ha puesto a disposición de los ciudadanos canales de comunicación para denunciar y alertar a las autoridades de personas y acciones sospechosas de pertenecer a grupos extremistas que se encuentran en su entorno.»⁸²⁴

Todo esto da cuenta del salto cualitativo y cuantitativo que realiza España con la adopción de la nueva Estrategia Nacional Contra el Terrorismo del año 2019, en donde se busca establecer la prevención por medio no solo de un modelo punitivo, sino también por medio de un modelo mecánico y primordialmente por medio de un modelo de prevención correctiva en donde participan no solo las instituciones jurídicas y policiales, sino también las instituciones educativas, medios de comunicación y otros actores del entramado social.

Ejemplos ilustrativos de este último enfoque preventivo comienzan a desarrollarse en España en todos los sectores de la sociedad. Dentro del ámbito académico, el Ayuntamiento de Málaga adopta el I Plan Transversal por la Convivencia y la Prevención de la Radicalización Violenta en la Ciudad de Málaga 2017-2020.⁸²⁵ La ciudad de Málaga es escogida por el Ministerio del

⁸²¹ Este tipo de orientaciones preventivas son parte de la calificación de Peter Lejins. De acuerdo con el autor, los modelos aplicados pueden determinar una prevención punitiva, una prevención correctiva o una prevención mecánica. Véase: VIRGINIA DEPARTMENT OF CRIMINAL JUSTICE SERVICES (2018), opus cit.

⁸²² «España defiende en la UE medidas conjuntas con empresas como Facebook o Twitter para combatir el yihadismo en la red», *Ibidem*.

⁸²³ Stop Radicalismos, *Ministerio del Interior. Gobierno de España*. Disponible en: <https://stop-radicalismos.ses.mir.es/stop/FormServlet> [Fecha de consulta: 24 de noviembre de 2023].

⁸²⁴ TOBOSO BUEZO, Mario (2016), opus cit., p. 4.

⁸²⁵ ANDRADE, Luis Julio/AYUNTAMIENTO DE MÁLAGA (2017): I Plan Transversal por la Convivencia y la Prevención de la Radicalización Violenta en la Ciudad de Málaga 2017-2020, elaborado por el Excmo. Ayuntamiento de Málaga y la Universidad de Málaga.

Interior como una ciudad piloto para la implementación de medidas de convivencia y tolerancia religiosa. La justificación de esta elección se desarrolla en torno a la tradicional multiculturalidad que siempre ha caracterizado a la ciudad por lo cual ha sido catalogada en muchas ocasiones como ejemplo de convivencia internacional, y que no obstante, no ajena a los radicalismos violentos a nivel global, encuentra la necesidad de profundizar el fomento a la unidad y la cohesión social mediante un equilibrio entre las identidades culturales de origen y la adopción de los valores fundamentales y las instituciones de la sociedad malagueña de acogida.⁸²⁶ Previamente la ciudad de Málaga, en mayo de 2016, se había posicionado como la primer ciudad de España en adherirse a la iniciativa *Strong Cities Network*⁸²⁷ creada por las Naciones Unidas.

En consonancia con este marco preventivo destacan las medidas de prevención correctiva que incluso comienzan a desarrollarse dentro del seno de propias instituciones policiales. Tal es el caso de la Policía de la Generalitat Mossos d'Esquadra, la cual ha desarrollado “un instrumento denominado PRODERAI (Protocolo de Detección de Radicalización Islamista) con el objetivo de prevenir y detectar procesos de radicalización violenta.”⁸²⁸ El instrumento PRODERAI está compuesto por tres niveles:

«PRODERAI Ejecución Penal: Los centros penitenciarios pueden constituir un entorno propicio para la radicalización. La prisión es un espacio con dinámicas sociales y psicológicas desvinculadas de las existentes en libertad. La consecuencia es que muchos cambios personales iniciados durante la privación de libertad no tienen continuidad cuando esta se recupera. En algunos supuestos la radicalización religiosa puede ser sincera, pero en otros puede ser adaptativa a la situación de internamiento ya sea para formar parte de un grupo, para hacerse respetar o como medida de evasión psicológica mientras dura el período de reclusión. El discernimiento y evaluación de cada caso es el objetivo de este nivel de acción.

PRODERAI Proximidad: Está destinado a aquellas unidades, grupos o agentes de los Mossos d'esquadra y de las Policías Locales que tiene un contacto más directo con los ciudadanos y las comunidades. La proximidad con el ciudadano proporciona a estos agentes un fiel conocimiento de la realidad social de su municipio. La proximidad se convierte en una oportunidad para detectar procesos de radicalización violenta.

PRODERAI Comunidad Educativa: Tiene como objetivos la prevención, la detección y la intervención de los procesos de radicalización islamista violenta en los centros educativos para preservar el crecimiento de los menores en un entorno tolerante. Proporciona orientación y recursos para la identificación de factores de riesgo que puedan propiciar la radicalización de los jóvenes. Tan sólo la culminación del proceso de radicalización violenta de un menor requerirá de la participación de otros actores como: la policía o la fiscalía de menores.»⁸²⁹

A excepción del primer nivel, en donde el foco de la prevención está determinado por el Derecho penal y las estructuras coercitivas del Estado, en este caso el sistema penitenciario, los dos niveles restantes del instrumento PRODERAI, dan cuenta de un nuevo enfoque transversal y evidencian la importancia de fundamentar el enfoque preventivo abordando la intervención

⁸²⁶ *Ibidem*, pág. 7.

⁸²⁷ Creada por las Naciones Unidas en el año 2015. El objetivo de esta red es ofrecer apoyo a ciudades para mejorar sus estrategias de prevención contra el extremismo violento, por medio del intercambio de información, aprendizaje mutuo e implementación de prácticas innovadoras en esta materia. Véase: Strong Cities Networks. Disponible en: <https://strongcitiesnetwork.org> [Fecha de consulta: 24 de noviembre de 2023].

⁸²⁸ TOBOSO BUEZO, Mario (2016), opus cit., p.4.

⁸²⁹ *Ibidem*, p 4-5.

ciudadana, los centros educativos, comunidades, y/o cualquier otro grupo o sector en donde existan personas o jóvenes susceptibles de radicalización.

En un ámbito exterior, es pertinente señalar que actualmente España colabora en un proyecto internacional denominado *Sawab. Unidos contra el Extremismo*⁸³⁰, cuya campaña comunicativa se orienta a crear un contradiscurso para deslegitimar⁸³¹ el aparato propagandístico de Dáesh en las redes sociales.

Según Fatima Lahnait, España ha desarrollado en los últimos años una estrategia de lucha contra el terrorismo en Internet cimentado en los programas PEV (Prevenir el Extremismo Violento) y la CEV (Combatir el Extremismo Violento). Según la autora,

«[...] A lo largo de las últimas dos décadas, la lucha contra el extremismo violento a nivel mundial ha consistido, sobre todo, en medidas antiterroristas basadas en la seguridad, adoptadas con el fin de reducir/disuadir/combater la amenaza que plantean los grupos extremistas violentos. Es desde hace tan solo unos pocos años que se aplican métodos más amplios e integrales para analizar los factores y causas por las que hay individuos que ingresan en grupos extremistas violentos.»⁸³²

España ha tomado buena cuenta de dichas innovaciones y las ha implementado dentro de su Política Criminal, sin abandonar por ello su tradicional enfoque punitivo y represivo del delito de terrorismo. No obstante, el uso de Internet por parte del yihadismo supone ponderar un elemento novedoso que orienta al Estado español a la implementación de modelos preventivos modernos, transversales, globales y armonizados con las orientaciones de la Unión Europea.

Podemos concluir parcialmente señalando que España utiliza el Derecho penal del enemigo para luchar contra los delitos de terrorismo, conforme posee dentro de su legislación penal un régimen especial que está fundado en determinadas excepciones constitucionales.

El sistema institucional de España tiende a centrarse especialmente en un modelo que otorga gran importancia a las medidas de securitización del Estado. Poseen especial importancia las unidades de investigación de la Policía Nacional y de la Guardia Civil, así como el CNI. Dentro de este marco, España tiende a desarrollar estrategias de seguridad orientadas al fortalecimiento de estas unidades, acrecentando sus competencias, infraestructura y formación en fuerzas de seguridad. Esta dotación se orienta a que su estructura sea más efectiva y coercitiva para combatir los delitos de terrorismo. El modelo preventivo es mixto porque cuenta con medidas punitivas (Derecho penal), medidas correctivas (P/CEV) y medidas mecánicas (cibervigilancia). Dentro del sistema de prevención otorga gran importancia a las medidas punitivas y mecánicas. Las medidas correctivas están siendo incorporadas en la última época, aunque todavía no han alcanzado un gran desarrollo en esta materia, y la prevención se orienta más a impedir la comisión del delito que a desarrollar campañas o asesorías orientadas a prevenir extremismo violentos. Esta visión más mecanicista y punitiva de la Política Criminal en España, nos permite englobarla dentro de *Warfare*, dado que desarrolla una lucha contra el terrorismo orientada en pie de guerra contra este fenómeno.

⁸³⁰ Sawab. Disponible en: <https://sawabcenter.org> [Fecha de consulta: 24 de noviembre de 2023].

⁸³¹ Dicha delimitación se promueve mediante la difusión de material audiovisual que ilustra las condiciones en las que viven los habitantes de los países que se encuentran bajo el régimen de la ocupación del autoproclamado Estado Islámico.

⁸³² LAHNAIT, Fatima (2021), opus cit., p. 45.

Tabla 6: Medidas de la Política Criminal de España respecto al delito de terrorismo.

TERRORISMO	ALEMANIA	REINO UNIDO	ESPAÑA
Derecho Penal	Derecho penal del ciudadano	Derecho penal del enemigo	De excepción (D. penal del enemigo)
Sistema Institucional	P/CEV	CONTEST	Seguritización
Modelo Preventivo	Mixto (punitivo, correctivo, mecánico)	Prevent	Mixto (punitivo, correctivo, mecánico)
Tendencia de la Política Criminal	Lawfare	Warfare	Warfare

Fuente: Elaboración propia. 2023.

CONCLUSIONES Y PROPUESTAS PARA FOMENTAR LA ARMONIZACIÓN DE LA POLÍTICA CRIMINAL EN LA UNIÓN EUROPEA EN MATERIA DE TERRORISMO EN INTERNET

CONCLUSIÓN N.º 1: LAS POLÍTICAS CRIMINALES DE ALEMANIA, REINO UNIDO Y ESPAÑA, EN CONSONANCIA CON LA UNIÓN EUROPEA, UTILIZAN LAS MEDIDAS NORMATIVAS, INSTITUCIONALES Y PREVENTIVAS PERO CADA ESTADO SE ORIENTA PRIORITARIAMENTE HACIA UNA DE ELLAS.

La política antiterrorista europea sin lugar a duda posee efectos en la Política Criminal de Alemania, de Reino Unido y de España, dado que la Unión Europea goza de una estructura política y normativa que le permite establecer no solo reglamentos y directivas de actuación, sino también su influencia.

No obstante, aun cuando desde el punto de vista formal existe una estructura supranacional que condiciona y subordina en muchos ámbitos el quehacer de los Estados europeos⁸³³, los mismos siguen manteniendo una cierta discrecionalidad en lo que respecta al desarrollo de su Política Criminal nacional con relación al delito de terrorismo.

Esto es así porque, a diferencia de lo que sucede con los delitos considerados comunes, el delito de terrorismo suscita en todos los Estados del Sistema internacional, discrepancias acerca de su tratamiento penal, policial/penitenciario, y preventivo.

Debido a ello, Alemania, Reino Unido y España poseen diferencias no solo con el resto de países del globo, sino también diferencias entre sí.

Sí bien las diferencias respecto al tratamiento de este delito son mayores con los Estados que no pertenecen a la región europea, prevalece dentro de Europa la noción de que todos los EEMM están comprometidos con la Política de Seguridad y Defensa Común (PSDC), y que ello implica la idea de que sus políticas criminales pueden o deberían de ser iguales.

Por lo tanto, que exista cierta discrecionalidad por parte de los Estados a la hora de abordar el terrorismo dentro de la región resulta relevante. En términos generales la Política Criminal de Alemania, Reino Unido y España orientada a su lucha contra el terrorismo es diferente.

Aun cuando estamos frente a Estados democráticos europeos que son fieles a los intereses de seguridad europea y a la defensa de los derechos fundamentales que impulsa la Unión, el delito de terrorismo presenta en general un tratamiento diferencial según de que Estado de trate.

Estas diferencias no son abismales fundamentalmente porque los Estados están vinculados entre sí por una organización internacional que posee lineamientos definidos en este sentido. Sin embargo, más allá de la ruta a seguir fijada por la UE, el Derecho penal interno, el tratamiento institucional, y el abordaje preventivo, dan cuenta de ejercicios autonómicos que exponen las orientaciones propias de cada Estado, para la punición, la represión y la prevención del delito de terrorismo.

⁸³³ Naturalmente, sí bien al presente Reino Unido no es un Estado miembro de la Unión Europea, no deja de estar en la órbita de la Unión Europea por intereses de defensa compartidos en la región.

El análisis de la Política Criminal de Alemania, Reino Unido y España nos permite conocer que:

1. La Política Criminal de Alemania y España, como Estados Miembros de pleno derecho de la Unión Europea sigue con mayor rigurosidad los lineamientos institucionales de la Unión. Por el contrario Reino Unido, mantiene con la Unión Europea una relación de mayor igualdad, no solo debido al hecho de que no se encuentra subordinado como ex EEMM a la organización internacional, sino primordialmente por el hecho de que suele estar a la vanguardia de la lucha antiterrorista. Debido a este motivo podría afirmarse que Reino Unido no sigue los lineamientos de la Unión Europea, sino que incluso es un actor proactivo que propone a la Unión Europea, opciones a considerar en la lucha contraterrorista. Un ejemplo de ello es la creación de la Unidad de Referencia de la UE (UE IRU) inspirada en el modelo británico.
2. Como ya hemos señalado en reiteradas ocasiones la Política Criminal está compuesta por medidas normativas, medidas institucionales u operativas y medidas preventivas. Alemania, Reino Unido y España promueven una Política Criminal nacional diferente entre sí, dado que cada país otorga especial importancia a un tipo de medida diferente. Esto bajo ningún aspecto significa restarle valor a los otros tipos de medidas, de hecho los tres Estados trabajan activamente en los tres campos de su Política Criminal. Sin embargo es posible identificar a que tipo de medida cada país otorga mayor importancia. Con relación a ello podríamos afirmar que:
 - a. La Política Criminal de Alemania se centra en las medidas preventivas: Alemania le otorga gran importancia a la legalidad de su Derecho penal, y al hecho de que el mismo no sufra deformaciones que pueden derivar en cuestionamientos por su antijuricidad. Por tal motivo, son fundamentales los rigurosos controles de constitucionalidad de las normas, a fin de que el Derecho penal alemán conserve sus virtudes garantistas. Alemania no ha creado un Derecho penal especial para combatir el terrorismo, sino que ha acumulado algunas excepciones dentro de su Derecho penal común, que son fuertemente cuestionadas. Debido a la negativa de este Estado de crear un Derecho penal especial y a los cuestionamientos sobre el Derecho penal de excepción que se ha ido creando *ad hoc*, Alemania apuesta fuertemente por el modelo preventivo. De los Estados analizados es el que posee la mayor variedad de programas preventivos gubernamentales y no gubernamentales, orientados a tratar toda forma de extremismo violento.
 - b. La Política Criminal de Reino Unido se centra en las medidas institucionales: Reino Unido es un Estado que se podría considerar a la vanguardia de la lucha contra el terrorismo, principalmente por su carácter anticipatorio en la búsqueda de erradicación del fenómeno. En su haber se encuentra una legislación especial antiterrorista, un gran aparato estatal de contraterrorismo y programas preventivos (*Prevent* y *Channel*) especiales. No obstante todas las medidas de Reino Unido (normativas, policiales y preventivas) poseen un criterio en común: son parte de una macroestructura institucional. Reino Unido nuclea el trabajo normativo, policial y preventivo bajo una dirección gubernamental/institucional.

El modelo preventivo de Reino Unido por ejemplo está estrictamente controlado por su Estrategia CONTEST, y su legislación especial es sometida a controles de constitucionalidad por un revisor independiente cuyo cargo ejecutivo resulta de una nueva función, incorporada como parte de la nueva Ley de Seguridad Nacional de 2023.⁸³⁴ El desarrollo y alcance de la normativa y el modelo preventivo británico está sujeto a la estructura institucional. El aparato institucional en Reino Unido es tan inmenso que excede las fuerzas policiales, las unidades de inteligencia o cuerpos penitenciarios habituales. En Reino Unido todo se institucionaliza en la lucha contra el terrorismo, y las medidas institucionales del Estado actúan como un gran paraguas que incorpora también las medidas legales y las medidas preventivas.

- c. La Política Criminal de España se centra en las medidas normativas: España promueve un permanente trabajo normativo. Tradicionalmente el tratamiento del terrorismo en España estuvo ligado a la punición, y se podría afirmar que se ha apostado fuertemente por el desarrollo de la vía punitiva para buscar reducir o eliminar el terrorismo en este Estado. Paralelamente España ha ido desarrollando también una infraestructura estatal integrada por unidades de inteligencia, que han nacido principalmente en el seno de los diversos Cuerpos y Fuerzas de Seguridad del Estado, con el consecuente acierto de estar integradas en instituciones reconocidas y legitimadas socialmente, pero con el desacierto de estar desvinculadas funcional y comunicativamente entre sí. Es decir, las diversas unidades de inteligencia de Ejército, Policía Nacional y/o Guardia Civil trabajan de forma colaborativa, pero no de forma integrada o institucionalizada. Otra de las dificultades que enfrenta España respecto a sus medidas institucionales es la escasez presupuestaria. De los tres Estados analizados, España es el país que menos recursos destina a su seguridad y defensa. Dentro de su Política Criminal, en el ámbito de las medidas institucionales ello se traduce en, por ejemplo, falta de infraestructura o capacitación para formar expertos propios en las unidades de inteligencia.⁸³⁵ Por otra parte, el trabajo desarrollado con medidas preventivas suele presentar esta misma carencia. Debido a ello las medidas normativas, por carecer de esta limitación presupuestaria, son las más desarrolladas en el país.

Está diferencia, aunque poco significativa en principio, atenta contra la búsqueda permanente de armonización de la Unión Europea respecto a la lucha contra el terrorismo. La Unión Europea

⁸³⁴ El revisor independiente es un cargo dentro de la estructura estatal de Reino Unido al que se accede por oposición pública. Véase: National Security Act 2023 (Ley de Seguridad Nacional de 2023). Disponible en: <https://www.legislation.gov.uk/ukpga/2023/32/contents> [Fecha de consulta: 29 de diciembre de 2023].

“El nuevo revisor independiente evaluará la justicia, eficacia y proporcionalidad de la legislación sobre amenazas estatales del Reino Unido e informará sus hallazgos y recomendaciones.” Actualmente el cargo es desempeñado por Jonathan Hall KC. Véase: «Independent Reviewer of State Threat Legislation appointed», *Home Office*. Disponible en: <https://www.gov.uk/government/news/independent-reviewer-of-state-threat-legislation-appointed#:~:text=It%20is%20a%20new%20role,report%20their%20findings%20and%20recommendations>. [Fecha de consulta: 29 de diciembre de 2023].

⁸³⁵ Por ejemplo, es habitual que dentro de las unidades de inteligencia se recurra a personas que no son miembros de los Cuerpos y Fuerzas de Seguridad del Estado para tareas de traducción en la red del idioma árabe, y que incluso en ocasiones se deba recurrir a nacionales de otros países que dominen el idioma de forma nativa.

aspira, como bloque regional, a mostrar al mundo una faceta de seguridad y defensa inquebrantable con la misma solidez que posee en el plano económico. El poderío económico de la Unión Europea no es cuestionable, no obstante, su capacidad defensiva hacia el exterior de sus fronteras, así como su seguridad interna se ha visto en ocasiones señalada. La Unión Europea busca minimizar estas diferencias que pudieran resultar en fisuras internas de su lucha contraterrorista.

CONCLUSIÓN N.º 2: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA DELEGA GRAN PARTE DE RESPONSABILIDAD HACIA EL SECTOR PRIVADO EN SU LUCHA CONTRA EL TERRORISMO YIHADISTA EN INTERNET.

En su lucha contra el yihadismo en Internet, la Unión Europea ha desarrollado un paquete de medidas de carácter normativo, operativo y preventivo que tienden al objetivo último de controlar y restringir los contenidos terroristas en la red. En este cometido, la Unión Europea no solo cuenta con el soporte de todas las instituciones de la UE, de sus agencias y de sus Estados Miembros, sino que también cuenta con la ayuda inestimable de sus socios, como son las empresas privadas de tecnología en Internet y los terceros Estados.

La Política Criminal de la Unión con relación a la lucha contra este crimen, se sostiene entonces sobre un tejido de actores, cuya continua colaboración e interacción permite asegurar la fiabilidad de una red digital europea ausente de contenidos terroristas propagandistas o violentos.

Referirnos a los actores intervinientes y modeladores de la Política Criminal de la UE nos remite necesariamente a la descripción que hemos realizado, en el desarrollo de esta tesis, acerca de los actores primarios y secundarios que diseñan la misma. Repasando dichos conceptos recordaremos que los actores primarios son aquellos que poseen capacidad de tomar decisiones adoptadas legítimamente por medio de diversas instancias formales e institucionales. Mientras que por medio de los actores secundarios se representan los intereses de la sociedad a través de los variados grupos de presión o sectores empresariales.

Las empresas de tecnología en Internet colaboran en las acciones que tienden al aseguramiento de la Europa digital, eso las posiciona como actor secundario de la Política Criminal de la UE, pero también como socio estratégico de la región.

Sin embargo, aun cuando en el entramado de actores intervinientes en esta gestión no se distingue un protagonismo claro entre todos los actores debido al hecho de que se trata de un trabajo altamente interrelacionado y cooperativo, los socios empresariales de la Unión, es decir, las empresas de tecnología de Internet sostienen una doble responsabilidad en cuanto al cumplimiento de sus funciones en el espacio europeo.

Por un lado, son percibidas por la Unión Europea como compañías a las que la Unión puede ayudar y con las que puede colaborar para erradicar el terrorismo yihadista en la red, pero por el otro, son observadas como empresas que deben de ser reguladas dentro del territorio europeo y sancionadas si sus plataformas no cumplen los estándares que garanticen la seguridad digital de la Unión.

Esto hace suponer que lejos de colaborar la Unión Europea con las empresas, son las empresas quienes tienen la real capacidad colaborar con la Unión y de restringir por tanto el flujo de contenido yihadista en Internet.

Sí bien naturalmente y de forma justa, la Unión se reserva para sí, mediante la aplicación de la DSA, el derecho a impedir que una empresa que no contribuya a garantizar la seguridad de la red no opere en el espacio comunitario; ello no significa necesariamente que no se dependa de forma voluntaria o regulada, de la acción de las empresas privadas. Como consecuencia, las empresas de tecnología en Internet acaban funcionando más como un actor primario de la Política Criminal de la Unión, que como un actor secundario. Ello deriva en una importante delegación de responsabilidad de los intereses en materia de seguridad de la Unión.

CONCLUSIÓN N.º 3: EN SU LUCHA CONTRA EL DELITO DE TERRORISMO YIHADISTA EN INTERNET, LA POLÍTICA CRIMINAL EUROPEA DEPENDE EN EXCESO DE LOS SISTEMAS JUDICIALES NACIONALES.

En un marco estatal las leyes del Estado tienden a redactarse lo más claramente posible para que las personas sean conscientes de sus responsabilidades y puedan tomar decisiones informadas acerca de sus acciones. En pocas palabras, las leyes claramente redactadas limitan la discrecionalidad y brindan protección contra la toma de decisiones inconsistentes o inapropiadas por parte de quienes tienen la tarea de implementar la ley.

En el ámbito de la Unión Europea sucede un hecho similar con los EEMM. En ausencia de un Derecho penal común, por medio del Derecho de la Unión, la UE confiere la tarea a los Estados de redactar en sus legislaciones internas leyes que permitan luchar de forma efectiva contra los delitos de terrorismo en Internet y privar de libertad a quienes incurren en este delito. Para ello orienta sus directivas, decisiones, reglamentos, etc., de tal forma que se reduzca al máximo la discrecionalidad otorgada a los Estados en esta materia. No obstante, habida cuenta de que no es tarea de la UE legislar sobre actos particulares criminales, la Organización Internacional queda encorsetada en las particularidades de cada EEMM respecto al tratamiento jurídico y penitenciario de estos delitos. Es evidencia de esto que la Unión aún no se ha puesto de acuerdo, en una sola declaración política, que es lo que considera como “actos criminales”, aunque por el contrario la UE resulta cada vez más taxativa en relación con lo que considera delito de terrorismo en Internet.

La legislación de la UE funciona bajo la premisa de que sus sanciones no son de naturaleza criminal. El Derecho penal de la UE actúa como un marco orientativo para los EEMM y requiere que el legislador europeo justifique sólidamente la criminalización. De ahí que existan innumerables declaraciones, protocolos, estrategias, etc., que describan la existencia de un peligro y establezcan el escenario requerido para que la UE inste a los EEMM a legislar sobre una materia penal determinada. Es decir, cualquier propuesta legislativa de la UE debe considerar antes por qué la UE debería legislar sobre una cuestión determinada.

No obstante, aun cuando las diversas acciones del terrorismo, o del terrorismo en Internet, no están tipificadas a nivel de la UE, son delitos que, cuando se tipifican a nivel nacional,

desencadenan el uso de procedimientos e instrumentos de cooperación policial y judicial en el marco de la UE, como por ejemplo la utilización de la Euroorden y el reconocimiento mutuo de sentencias judiciales.

El sistema de orden de detención europea ha revolucionado la eficacia de la cooperación policial transfronteriza, pero también ha llamado la atención sobre las disparidades entre los sistemas penales nacionales de los EEMM. Por ejemplo, el reconocimiento mutuo de sentencias requiere una confianza mutua que a su vez está condicionada a la creencia de que todos los sistemas de justicia penal de los EEMM satisfacen estándares mínimos. Sin embargo, diversos autores⁸³⁶ demuestran que a menudo esto no es así. También sucede algo similar con transposiciones incompletas. Todo ello genera un desequilibrio no solo entre los Estados, sino primordialmente dentro de la Unión, que en la lucha para perseguir el crimen de terrorismo en Internet se materializa en una merma de su capacidad para lograr su objetivo.

El Derecho penal de la UE sigue estando incómodamente situado entre el derecho internacional y el nacional. Los instrumentos del Derecho penal de la UE luchan por desarrollar efectos jurídicos autónomos, dado que actualmente la legislación de la UE es aplicable en los EEMM, pero sólo muy excepcionalmente tiene efecto directo en procedimientos contra particulares. Ello implica que el Derecho penal de la Unión continúe siendo imperfecto bajo los acuerdos actuales, en parte debido a la dependencia que tiene la UE de la legislación de los sistemas judiciales nacionales.

Todo esto lleva a la conclusión de que parte del Derecho penal de la UE es un “Derecho penal virtual”⁸³⁷ que no se legisla ni se aplica a nivel nacional. Según Miettinen, si no existe una ley común de implementación, ¿constituye este derecho europeo una declaración de la Política Criminal de la UE? La duda es razonable, no obstante, podemos decir que sí, y que las orientaciones de la Política Criminal europea son precisamente aquellas que poseen influencia en el derecho interno de los Estados Miembros.

Ahora bien, esa influencia que ejerce el DUE en los EEMM es necesaria precisamente por la dependencia que posee la Unión Europea de los derechos internos. De ahí que la armonización de las legislaciones sea el mejor instrumento que la Unión posee en el ámbito legislativo. La armonización de las legislaciones penales nacionales permite que la Política Criminal de la UE no posea una dependencia nociva o contraria a sus propios intereses.

Por ello, en el afán de fomentar aún más la armonización legislativa en la lucha contra el terrorismo yihadista en Internet, las orientaciones europeas deben de ser claras y deben de depositar en los EEMM la responsabilidad del cumplimiento de los criterios y estándares de la UE, así también como reconocer el desempeño individual y el mérito nacional de una legislación exitosa y apegada a los criterios generales de Europa.

⁸³⁶ MORILLAS CUEVA, Lorenzo/VALLS PRIETO, Javier (2006): «Hacia la nueva realidad de un Derecho penal europeo», *Revista de la Facultad de Derecho de la Universidad de Granada*, núm. 9, p. 181.

⁸³⁷ MIETTINEN, Samuli (2013): *Criminal Law and Policy in the European Union*. London: Routledge, p. 6.

CONCLUSIÓN N.º 4: LAS DISCREPANCIAS PRESUPUESTARIAS, EL AUGE DE LOS NACIONALISMOS Y LA FALTA DE VOLUNTAD POLÍTICA DE LOS ESTADOS MIEMBROS REPRESENTAN UNA AMENAZA PARA LA POLÍTICA CRIMINAL DE LA UE EN SU LUCHA CONTRA EL TERRORISMO EN INTERNET.

Según el Índice Global de Terrorismo de 2018 (GTI),⁸³⁸ a partir del periodo 2016-2017, Europa comenzó una paulatina mejoría, respecto al resto de regiones analizadas, en lo referente a la protección contra el terrorismo. En este periodo, a la luz de los índices evaluados, el informe consigna que la seguridad europea aumentó y mejoró considerablemente. Por ejemplo, se ha registrado una disminución en el número de víctimas mortales del terrorismo, que se traduce en un 50% menos de víctimas cada año. No obstante, sí bien esa es la tendencia, estas cifras no se dan por igual en toda la región. Mientras que en Alemania, Bélgica, Francia y Turquía se registraron importantes disminuciones de los atentados, en Austria, España, Finlandia, Reino Unido y Suecia se ha registrado un aumento de las acciones terroristas.

Esta realidad es un enorme logro si se tienen en consideración todos los problemas que existen dentro de la Unión y que resultan una amenaza para el logro de sus objetivos.

Los esfuerzos que realiza la Unión Europea para mantener los índices del delito de terrorismo lo más reducido posible son muy altos, porque la Política Criminal de la Unión debe hacer frente a la lucha contra el terrorismo en Internet, a la vez que debe resolver problemas internos.

Uno de los problemas internos de la Unión Europea es el relacionado con el presupuesto que cada EEMM asigna a la seguridad y defensa común. Si bien existe la CARD⁸³⁹ que coordina los esfuerzos presupuestarios de la Unión a fin de que exista un equilibrio en esta materia entre todos los EEMM, lo cierto es persisten las diferencias. Estas diferencias presupuestarias que tienen lugar entre los diferentes Estados de la UE afectan a la Política Criminal europea, y acaban por debilitarla.

Otro de los problemas internos que enfrenta la Política Criminal es el surgimiento de los nacionalismos. Los nacionalismos europeos, intensificados en los últimos diez años, han llevado a cuestionar la existencia misma de la Unión Europea por parte de los sectores más radicales de algunos Estados, y a poner en duda su eficacia para luchar contra el terrorismo. Finalmente, todo este panorama ha desmotivado al conjunto de los Estados europeos y ha afectado la voluntad política de los miembros de la Unión para operar de forma comunitaria con elevado éxito.

Estas amenazas, que han nacido dentro de la propia Unión, no solo han afectado al funcionamiento común de la Unión Europea, sino que también han potenciado las diferencias previas entre los EEMM en materia de seguridad. De esta forma, algunos Estados, en aras de mantener garantizada la seguridad dentro de sus fronteras nacionales, comenzaron a desarrollar medidas internas como desarrollar una legislación más punitiva o promover el incremento del presupuesto interno para defensa.

⁸³⁸ INSTITUTE FOR ECONOMICS & PEACE (2018): *Global Terrorism Report 2018: Measuring and understating the impact of terrorism*, Sydney, November 2018. Disponible en: <http://visionofhumanity.org/reports> [Fecha de consulta: 22 de noviembre de 2023].

⁸³⁹ Revisión Anual Coordinada de la Defensa (CARD, *Coordinated Annual Review on Defence*) englobada en la Estrategia Global de la UE desarrollada por la Agencia Europea de Defensa (EDA, European Defense Agency). La CARD realiza un seguimiento de los planes de defensa de los EEMM y ayuda a coordinar el gasto e identificar posibles proyectos de colaboración.

Los terroristas han sabido aprovechar las diferencias internas de los países. Han comprendido rápidamente que, si un Estado les impide desarrollar sus actividades, simplemente deben trasladarse a otro. Si bien las acciones terroristas se realizan en Internet, el tratamiento del crimen puede ser muy diferente de un Estado a otro. Por ello, desde la perspectiva yihadista, Internet se ha transformado en el refugio virtual que desafía las fronteras nacionales, no sólo físicas, sino primordialmente aquellas que nacen de las diferencias entre los propios Estados de la Unión.

Es menester tratar de reducir al máximo estos problemas dentro de la Unión Europea que atentan contra la seguridad y la defensa conjunta. Mientras persistan estas tensiones de carácter interno se verá amenazada la solidez de la Política Común de Seguridad y Defensa (PCSD). Como hemos dicho en más de una ocasión a lo largo de esta tesis, el problema del terrorismo en Internet no puede ser únicamente abordado con medidas militares, sino que requiere de un enfoque multidisciplinario. La defensa colectiva y la respuesta unificada frente al terrorismo resulta imprescindible. La seguridad y la defensa deben ser conceptos vinculados y no debe ni puede concebirse la idea de mantener la seguridad sin tener una capacidad defensiva conjunta. El desafío de la Política Criminal de la Unión Europea está en que las amenazas provengan únicamente del terrorismo.

La Unión Europea ha sabido anticipar estos peligros internos y en 1994 estableció el Comité Europeo de las Regiones.⁸⁴⁰ Este Comité busca reducir las diferencias existentes entre los Estados de la Unión, otorgando voz a las regiones y ciudades de Europa de forma consultiva para que evalúen a priori el impacto que pueden tener determinadas medidas europeas en dichas regiones y ciudades. Esta acción no solo tiende a disminuir las diferencias entre las regiones, sino fundamentalmente a armonizar las políticas normativas, operativas o preventivas para que encuentren menos resistencia en su aplicación.

Europa debería de incentivar este tipo de medidas que no están orientadas al establecimiento de normas jurídicas o a políticas criminológicas, sino al reconocimiento mutuo de la identidad cultural. Este modelo de gestión institucional es un buen ejemplo de cómo se puede ayudar a amortiguar las diferencias entre las regiones y cómo ayudar a crear un escenario más positivo para aceptar de mejor grado las medidas comunitarias.

CONCLUSIÓN N.º 5: LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA ES REACTIVA, NO PROACTIVA.

En términos generales parece suceder que la Unión Europea y los EEMM han adquirido conciencia del problema del terrorismo internacional de forma tardía. Naturalmente esto no es así, como hemos afirmado en más de una ocasión, el problema del terrorismo ha sido una constante en el territorio europeo que obligó a la región a actuar con referencia a esta materia de forma temprana. Las innumerables políticas, estrategias, etc., que se han implementado dan

⁸⁴⁰ El Comité Europeo de las Regiones (CDR) representa a los entes locales y regionales de toda la Unión Europea. El CDR interviene en distintas fases del proceso legislativo de la UE. Las comisiones del CDR elaboran dictámenes sobre las propuestas legislativas de la UE y los miembros se reúnen en el pleno para votar y aprobar estos dictámenes. Véase: Comité Europeo de las Regiones. Disponible en: <https://cor.europa.eu/es> [Fecha de consulta: 22 de noviembre de 2023].

cuenta de que para la Unión Europea el problema del terrorismo, y posteriormente el fenómeno del terrorismo yihadista, y el terrorismo yihadista en Internet, ha sido siempre una prioridad.

Ahora bien, esta prioridad se ha caracterizado en analizar mediante informes de expertos los efectos de los actos terroristas y de sus acciones delictivas previas o derivadas, y en orientar a los EEMM en cuanto a las prioridades de la Unión en esta materia.

Ello significa que la Unión se ha focalizado en limitar los delitos del terrorismo yihadista en Internet, pero no se ha centrado en desarrollar un modelo de análisis anticipatorio de las posibles acciones terroristas en la red. La legislación europea también ha actuado de forma similar, y da cuenta de propuestas jurídicas del problema a posteriori. Evidencia de ello es que no existen reglamentos, decisiones o directivas tendientes a proteger, de forma previa al hecho delictivo, el espacio digital europeo.

Este enunciado no significa bajo ningún aspecto proponer una punición sobre un hecho delictivo que no ha tenido lugar, sino que manifiesta la necesidad de legislar en materia penal a priori de la comisión de un delito de forma preventiva.

Por ejemplo, en 1969 tuvo lugar la aparición de Internet de la mano de Arpanet. Casi treinta años más tarde, aproximadamente en 1998, tuvo lugar la democratización de Internet que significó que Internet se convirtiese en un canal de comunicación masivo y global, y en el año 2001 Internet fue utilizado por el yihadismo para promover propaganda terrorista. Tuvieron que pasar tres años más desde el uso masivo de Internet hasta la primera comunicación realizada en la red por el terrorismo⁸⁴¹. Pensar de forma preventiva significaría haber “pensado Internet”, cuando su surgimiento, como un nuevo espacio posible para la comisión delictiva del terrorismo, y entonces poder así instrumentalizar los medios para evitar la comisión de delitos en el nuevo escenario virtual. Un inciso aparte merece el Convenio sobre la Ciberdelincuencia del año 2001.⁸⁴² Este documento de extrema importancia significó tempranamente un hito en la observancia de Internet como un nuevo escenario delictivo. Sin embargo, primero, el Convenio sobre Ciberdelincuencia no pertenece a la Unión Europea, sino al Consejo de Europa lo que significaría que este organismo externo a la Unión ha sabido ver, de forma más proactiva que la propia Unión, los peligros futuros de Internet como escenario novedoso del crimen; y segundo, tuvo lugar una vez perpetrados los ataques del 11-S.

No debe dejarse de lado por tanto la importancia que tiene el hecho de pensar creativamente sobre los nuevos escenarios y espacios de oportunidad para el crimen. No debe olvidarse que esa misma temporalidad, desde 1998 a 2001, es la que ha tenido el terrorismo yihadista, quien en este caso en menos de tres años ha realizado el aprovechamiento de un nuevo canal comunicativo y lo ha convertido en un nuevo escenario del delito.

La cooperación europea para la vigilancia en Internet y la represión sobre su uso con fines yihadistas ha ido paulatinamente estableciéndose de forma sólida y especializada. Actualmente, la Política Criminal europea en este ámbito se centra en la cooperación para la erradicación de contenido violento en la red, y este objetivo se ha transformado en un elemento de vital importancia que integra la actual lucha antiterrorista. Sin embargo, la cooperación europea

⁸⁴¹ Se refiere a los mensajes vertidos en la red con antelación al 11/9, en los que Al Qaeda advertía de un ‘ataque inminente y a gran escala’ a Estados Unidos. Véase: WEIMANN, Gabriel (2004), opus cit., p. 3.

⁸⁴² CONSEJO DE EUROPA (2001), opus cit.

siempre ha tenido lugar posteriormente a la identificación de hechos delictivos consumados, y nunca frente a la idea de una amenaza latente.

Resulta evidente y necesario reforzar el pilar de la prevención a fin de anticiparse a posibles crisis futuras que pueda deparar la existencia del terrorismo en Internet. Es decir, es urgente y fundamental preparar enfoques creativos multilaterales y multidisciplinarios que permitan anticipar amenazas y escenarios aún no acontecidos.

La naturaleza de combatir una amenaza radica en el hecho de combatir algo aún no concretado⁸⁴³, pero que posee una gran potencialidad de materialización. Si el actual enfoque europeo está combatiendo fenómenos que están en nuestra sociedad, significa que la lucha antiterrorista está enfocada en erradicar situaciones ya claramente asentadas.

Por supuesto que esto es necesario y lógico, y a su vez permite la existencia de una Política Criminal eficaz en el cumplimiento de su objetivo de reducción del crimen. Pero, podríamos fomentar un trabajo pleno que fortalezca la Política Criminal de la Unión, si ésta procurara anticiparse y prevenir las futuras acciones del terrorismo en la red, y no solo centrarse en reducir la tasa de los crímenes actuales.

Debido a esta realidad descrita, podemos afirmar que la Política Criminal de la Unión Europea ha tendido tradicionalmente a ser reactiva, y no proactiva. Es decir, a reaccionar a los hechos delictivos del terrorismo en Internet, sin anticiparse a nuevos acontecimientos.

En un intento de cambiar esta dinámica habitual, en el año 2020 tuvo lugar la creación de la *Estrategia de la Unión de la Seguridad de la UE*,⁸⁴⁴ que estará vigente hasta el año 2025. Por vez primera, en un documento estratégico de la UE, se detallan ámbitos prioritarios en la lucha contra el terrorismo que dan cuenta de una visión preventiva, debido a que aún no han acontecido. Se hace referencia en el documento citado a las amenazas híbridas y a la necesidad de incrementar la resiliencia de las infraestructuras críticas de la Unión, debido a que se estima que el terrorismo yihadista en Internet se moverá desde el cibercrimen hacia la ciberguerra.

Sin embargo, este cambio de categoría de cibercrimen a ciberguerra, definido por probables ataques sistemáticos futuros a infraestructuras de la UE y por el bioterrorismo⁸⁴⁵ ha sido propuesto por Estados Unidos en el año 2017⁸⁴⁶, lo que significa que Europa sigue sosteniendo dentro de su Política Criminal, una línea discursiva que requiere ser justificada por hechos delictivos presentes o legitimada por EEUU.

Es necesario seguir investigando acerca de las futuras tendencias de la radicalización extrema del yihadismo, y evaluar no solo las prácticas y amenazas criminales del terrorismo presente en Internet, sino las probables y futuras para una intervención preventiva y proactiva.

⁸⁴³ No se refiere bajo ningún aspecto a punición anticipada, o a un adelantamiento de la barrera penal, sino a la anticipación de los escenarios del crimen.

⁸⁴⁴ COMISIÓN EUROPEA (2020), opus cit.

⁸⁴⁵ Terrorismo cometido por medio de armas de destrucción masiva de carácter químico, biológico, radiológico y nuclear, cuya planeación, coordinación y ejecución pueden cometerse por medio de sistemas de cómputo y de forma remota.

⁸⁴⁶ UNITED NATIONS OFFICE OF COUNTER-TERRORISM (2017): *Ensuring Effective Interagency Interoperability and Coordinated Communication in Case of Chemical and/or Biological Attacks*. New York: United Nations Headquarters.

CONCLUSIONS AND PROPOSALS TO PROMOTE THE HARMONIZATION OF CRIMINAL POLICY IN THE EUROPEAN UNION REGARDING TERRORISM ON THE INTERNET

CONCLUSION N.º 1: THE CRIMINAL POLICIES OF GERMANY, THE UNITED KINGDOM AND SPAIN, IN STUNNING WITH THE EUROPEAN UNION, USE REGULATORY, INSTITUTIONAL AND PREVENTIVE MEASURES BUT EACH STATE IS PRIORITY ORIENTED TOWARDS ONE OF THEM.

The European anti-terrorist policy has effects on the Criminal Policy of Germany, the United Kingdom and Spain, because the European Union has a political and regulatory structure that allows it to establish not only regulations and directives for action, but also influence.

However, even when there is a supranational structure that conditions and subordinates the work of European States⁸⁴⁷, these European States have some autonomy in establishing their national Criminal Policy in relation to the crime of terrorism.

This is because, unlike what happens with crimes considered common, the crime of terrorism has differences in its criminal, police/penitentiary, and preventive treatment in all States of the international system.

For this reason, Germany, the United Kingdom and Spain have differences not only with the rest of the countries on the globe, but also differences between themselves.

The differences regarding the treatment of this crime are greater with the States that do not belong to the European Union. Within Europe, the idea prevails that all Member States are committed to the Common Security and Defense Policy (CSDP), and this means the idea that their criminal policies can or should be the same.

Therefore, the fact that there are differences in the States regarding the treatment of terrorism within the Union is relevant.

In general terms, the Criminal Policy of Germany, the United Kingdom and Spain in their fight against terrorism is different.

Even when we are dealing with European democratic States that are faithful to European security interests and the defense of fundamental rights promoted by the Union, the crime of terrorism generally presents differential treatment depending on which State is involved. These differences are not abysmal fundamentally because the States are linked to each other by an international organization that has defined guidelines in this regard. However, beyond the route set by the EU, domestic criminal law, institutional treatment, and preventive approach, has the autonomy of each State, for the punishment, repression and prevention of the crime of terrorism.

The analysis of the Criminal Policy of Germany, the United Kingdom and Spain allows us to know that:

⁸⁴⁷ Naturally, although the United Kingdom is not currently a Member State of the European Union, it is still in the orbit of the European Union due to shared defense interests in the region.

1. The Criminal Policy of Germany and Spain, as full Member States of the European Union, rigorously follows the institutional guidelines of the Union. In an opposite sense, the United Kingdom maintains a relationship of greater equality with the European Union, not only because it is not subordinated as a former Member State to the international organization, but fundamentally because it is usually at the forefront of the anti-terrorist fight. For this reason, it can be said that the United Kingdom does not follow the guidelines of the European Union, and that it is even a proactive actor that proposes to the European Union options to consider in the fight against terrorism. An example of this is the creation of the EU Reference Unit (EU IRU) inspired by the British model.
2. As we have already pointed out on numerous occasions, the Criminal Policy is made up of regulatory measures, institutional or operational measures and preventive measures. Germany, the United Kingdom and Spain promote a different national Criminal Policy from each other, given that each country gives special importance to a different type of measure. This in no way means to detract from the other types of measures; in fact, the three States work actively in the three fields of their Criminal Policy. However, it is possible to identify which type of measure each country gives greater importance to. In relation to this we could affirm that:
 - a. Germany's Criminal Policy focuses on preventive measures: Germany places great importance on the legality of its criminal law, and on the fact that it does not suffer legal distortions. For this reason, demanding controls on the constitutionality of the rules are essential, so that German criminal law preserves its guarantees. Germany has not created a special criminal law to combat terrorism but has accumulated some exceptions within its common criminal law, which are strongly questioned. Due to the refusal of this State to create a special criminal law and the questions about the exceptional criminal law that has been created ad hoc, Germany is strongly committed to the preventive model. Of the States analyzed, it is the one that has the greatest variety of governmental and non-governmental preventive programs, aimed at treating all forms of violent extremism.
 - b. The United Kingdom's Criminal Policy focuses on institutional measures: the United Kingdom is a State that could be considered at the forefront of the fight against terrorism, mainly due to the anticipatory nature in the search for the eradication of this phenomenon. It has special anti-terrorist legislation, a large state counterterrorism apparatus and special preventive programs (Prevent and Channel). However, all the United Kingdom measures (regulatory, police and preventive) have a common criterion: they are part of an institutional macrostructure. The United Kingdom brings together regulatory, police and preventive work under government/institutional direction. The United Kingdom's preventive model, for example, is strictly controlled by its CONTEST Strategy, and its special legislation is subject to constitutionality checks by an independent reviewer whose executive position results from a new function, incorporated as part of the new National

Security Law of 2023.⁸⁴⁸ The development and scope of the British regulations and preventive model is subject to the institutional structure. The institutional framework in the United Kingdom is so immense that it exceeds the usual police forces, intelligence units or penitentiary bodies. In the United Kingdom, everything is institutionalized in the fight against terrorism, and the institutional measures of the State act as a large umbrella that also incorporates legal measures and preventive measures.

- c. Spain's Criminal Policy focuses on regulatory measures: Spain promotes permanent regulatory work. Traditionally, the treatment of terrorism in Spain was linked to punishment, and it could be stated that there has been a strong commitment to punitive means to reduce or eliminate terrorism in this State. At the same time, Spain has also been developing an infrastructure made up of intelligence units, which have been created mainly in the State Security Corps and Forces, with the success of being integrated into recognized and legitimized institutions, but with the mistake of not being functionally and communicatively linked with each other. The various intelligence units of the Army, National Police and/or Civil Guard work in a collaborative manner, but not in an integrated or institutionalized manner. Another of the difficulties that Spain faces regarding its institutional measures is the budgetary difficulty. Of the three States analyzed, Spain is the country that provides the smallest budget for its security and defense. In its Criminal Policy, in the field of institutional measures this means lack of infrastructure or training of own experts in the intelligence units.⁸⁴⁹ On the other hand, work carried out with preventive measures usually presents this same deficiency. For this reason, the regulatory measures, because they do not have budgetary limitations, are the most developed in this country.

This difference affects the permanent search for harmonization of the European Union regarding the fight against terrorism. The European Union aspires, as a regional organization, to show the world a face of unbreakable security and defense with the same solidity that it has on the economic level.

The economic power of the European Union is not debatable, however, its defensive capacity as well as its internal security has often been questioned. The European Union seeks to minimize these differences that could result in internal fissures in its fight against terrorism.

⁸⁴⁸ The independent reviewer is a position within the United Kingdom state structure that is accessed by public competition. See: National Security Act 2023. Available in: <https://www.legislation.gov.uk/ukpga/2023/32/contents> [Consultation date: December 29, 2023].

“*The new independent reviewer will assess the fairness, effectiveness and proportionality of the UK’s state threat legislation and report its findings and recommendations.*” The position is currently held by Jonathan Hall KC. See: «Independent Reviewer of State Threat Legislation appointed», *Home Office*. Available in: <https://www.gov.uk/government/news/independent-reviewer-of-state-threat-legislation-appointed#:~:text=It%20is%20a%20new%20role,report%20their%20findings%20and%20recommendations>. [Consultation date: December 29, 2023].

⁸⁴⁹ For example, it is common that within intelligence units people who are not members of the State Security Corps and Forces are used for translation tasks from the Arabic language, and that sometimes citizens of other countries must even be used.

CONCLUSION N.º 2: THE CRIMINAL POLICY OF THE EUROPEAN UNION DELEGATES A LARGE PART OF RESPONSIBILITY TO THE PRIVATE SECTOR IN ITS FIGHT AGAINST JIHADIST TERRORISM ON THE INTERNET.

In its fight against jihadism on the Internet, the European Union has developed a package of regulatory, operational and preventive measures that tend to the ultimate objective of controlling and restricting terrorist content on the Internet. In this task, the European Union not only has the support of all the EU institutions, its agencies and its Member States, but also has the invaluable help of its partners, such as private Internet technology companies and third States. The Union's Criminal Policy in relation to the fight against this crime is based on a network of actors, whose collaboration and interaction makes it possible to ensure the European digital network is free of propagandistic or violent terrorist content.

Naming the actors of the EU Criminal Policy necessarily refers us to the description that we have made, in the development of this thesis, about the primary and secondary actors that design the Criminal Policy. Reviewing these concepts, we will remember that the primary actors are those who have the capacity to make decisions adopted legitimately through various formal and institutional instances. While through secondary actors the interests of society from the various pressure groups or business sectors are represented.

Internet technology companies collaborate in actions that lead to a safe digital Europe, which positions them as a secondary actor in the EU's Criminal Policy, but also as a strategic partner of the region.

Even though the network of actors involved in EU Criminal Policy does not distinguish a clear role among all actors because it is a highly interrelated and cooperative work, Internet technology companies have a double responsibility. regarding the fulfillment of its functions in the European space.

On the one hand, they are perceived by the European Union as companies that the Union can help and with which it can collaborate to eradicate jihadist terrorism on the Internet, but on the other hand, they are observed as companies that must be regulated within the European territory and sanctioned if their platforms do not meet the standards that guarantee the digital security of the Union.

This suggests that far from the European Union collaborating with companies, it is the companies who have the real ability to collaborate with the Union and restrict jihadist content on the Internet.

The Union reserves for itself, through the application of the DSA, the right to refuse to allow a company that does not contribute to ensuring network security to operate in the Community space. But this does not mean that there is no voluntary or regulated dependence on the actions of private companies. Therefore, Internet technology companies act more as a primary actor in the Union's Criminal Policy, rather than as a secondary actor. This results in an important delegation of responsibility for the security interests of the Union.

CONCLUSION N.º 3: IN ITS FIGHT AGAINST THE CRIME OF JIHADIST TERRORISM ON THE INTERNET, EUROPEAN CRIMINAL POLICY DEPENDS OVERLY ON NATIONAL JUDICIAL SYSTEMS.

In a state framework, state laws tend to be written as clearly as possible so that people are aware of their responsibilities and can make informed decisions about their actions. Simply put, clearly written laws limit discretion and provide protection against inconsistent or inappropriate decision making by those tasked with implementing the law.

At the level of the European Union, a similar event occurs with the Member States. In the absence of a common criminal law, through Union Law the EU confers the task on the States of drafting in their domestic legislation laws that allow them to effectively fight against terrorist crimes on the Internet and deprive of freedom of those who commit in this crime. To this end, it develops its directives, decisions, regulations, etc., in such a way that the discretion granted to States in this matter is reduced to a maximum. However, given that it is not the EU's task to legislate on criminal acts, the International Organization is limited by the particularities of each Member State regarding the legal and penitentiary treatment of these crimes.

Evidence of this is that the Union has not yet agreed on a single political declaration, on what it considers "criminal acts", although on the contrary the EU is becoming more and more restrictive in relation to what it considers terrorism on the Internet.

EU law operates on the premise that its sanctions are not criminal. EU criminal law acts as a guiding framework for Member States and requires the European legislator to provide solid justifications for criminalization. For this reason, there are countless declarations, protocols, strategies, etc., that describe the existence of a danger and establish the required scenario for the EU to urge the Member States to legislate on a specific criminal matter. In other words, any EU legislative proposal must first consider why the EU should legislate on a given issue.

However, even though the various actions of terrorism, or terrorism on the Internet, are not classified at EU level, they are crimes that, when classified at national level, trigger the use of procedures and instruments of police and judicial cooperation. For example, in the EU, the Euroorder and the mutual recognition of judicial rulings.

The European arrest warrant system has revolutionized the effectiveness of cross-border police cooperation but has also drawn attention to the disparities between the national criminal systems of the Member States. For example, mutual recognition of sentences requires mutual trust which in turn is conditioned on the belief that all criminal justice systems in the Member States satisfy minimum standards. However, various authors⁸⁵⁰ show that this is often not the case. Something similar also happens with incomplete transpositions. All of this generates an imbalance not only between the States, but primarily within the Union. In the fight to prosecute terrorism on the Internet this means a reduction in its ability to achieve its objective.

⁸⁵⁰ MORILLAS CUEVA, Lorenzo/VALLS PRIETO, Javier (2006): «Hacia la nueva realidad de un Derecho penal europeo», *Revista de la Facultad de Derecho de la Universidad de Granada*, n.º. 9, p. 181.

EU criminal law remains uncomfortably situated between international and national law. The instruments of EU criminal law struggle to develop autonomous legal effects, given that EU legislation is currently applicable in the Member States, but only very exceptionally has it direct effect in proceedings against individuals. This means that the Union's criminal law remains imperfect under current agreements, partly due to the EU's dependence on the legislation of national judicial systems.

All this leads to the conclusion that part of EU criminal law is “virtual criminal law”⁸⁵¹ that is not legislated or applied at national level. According to Miettinen, if there is no common implementing law, does this European law constitute a declaration of the EU Criminal Policy? The doubt is reasonable, however, we can say yes, and that the guidelines of the European Criminal Policy are precisely those that influence the domestic law of the Member States.

Now, this influence that the DUE exercises in the Member States is necessary precisely because of the dependence that the European Union has on internal rights. Hence, the harmonization of legislation is the best instrument that the Union has in the legislative field. The harmonization of national criminal legislation allows the EU Criminal Policy to not have a harmful or contradictory dependence on its own interests.

Therefore, to further promote legislative harmonization in the fight against jihadism on the Internet, European guidelines must be clear and must be deposited in the Member States. Likewise, it must also recognize the individual performance and national merit of successful legislation that adheres to the general criteria of Europe.

CONCLUSION N.º 4: BUDGET DISCREPANCIES, THE RISE OF NATIONALISM AND THE LACK OF POLITICAL WILL OF THE MEMBER STATES ARE A THREAT TO THE EU'S CRIMINAL POLICY IN ITS FIGHT AGAINST TERRORISM ON THE INTERNET.

According to the 2018 Global Terrorism Index (GTI),⁸⁵² starting from the 2016-2017 period, Europe began a gradual improvement, compared to the rest of the regions analyzed, in terms of protection against terrorism. In this period, the report details that European security increased and improved considerably. For example, there has been a decrease in the number of fatalities from terrorism, which translates into 50% fewer victims each year. However, although this is the trend, these figures are not the same throughout the region. While significant decreases in attacks were recorded in Germany, Belgium, France and Turkey, an increase in terrorist actions has been recorded in Austria, Spain, Finland, the United Kingdom and Sweden.

⁸⁵¹ MIETTINEN, Samuli (2013): *Criminal Law and Policy in the European Union*. London: Routledge, p. 6.

⁸⁵² INSTITUTE FOR ECONOMICS & PEACE (2018): *Global Terrorism Report 2018: Measuring and understating the impact of terrorism*, Sydney, November 2018. Available in: <http://visionofhumanity.org/reports> [Consultation date: November 22, 2023].

This reality is an enormous achievement if we take into consideration all the problems that exist within the Union and that are a threat to the achievement of its objectives.

The efforts made by the European Union to keep terrorism crime rates as low as possible are very high because the Union's Criminal Policy must fight against terrorism on the Internet, at the same time as it must resolve internal problems.

One of the internal problems of the European Union is related to the budget that each Member State allocates to common security and defense. Although there is the CARD⁸⁵³ that coordinates the budgetary efforts of the Union to have a balance in this matter between all the Member States, the truth is that differences persist. These budgetary differences that take place between the different EU States affect the European Criminal Policy and end up weakening it.

Another of the internal problems that Criminal Policy faces is the emergence of nationalisms. European nationalism, intensified in the last ten years, has led the most radical sectors of some States to question the very existence of the European Union, and to question its effectiveness in fighting terrorism. Finally, this entire panorama has demotivated all European States and has affected the political will of the members of the Union to operate as a community with great success.

These threats, which have arisen within the Union itself, have not only affected the common functioning of the European Union, but have also increased previous differences between the Member States in terms of security. In this way, some States, to maintain guaranteed security within their national borders, began to develop internal measures such as developing more punitive legislation or promoting an increase in the internal budget for defense.

Terrorists have known how to take advantage of the internal differences of countries. They have quickly understood that, if a State prohibits them from carrying out their criminal activities, they must simply move to another. Although terrorist actions are carried out on the Internet, the treatment of crime can be very different from one State to another. For this reason, from the jihadist perspective, the Internet has become the virtual refuge that challenges national borders, not only physical, but primarily those that arise from the differences between the States of the Union themselves.

It is necessary to try to reduce as much as possible these problems within the European Union that threaten security and joint defense. If these internal tensions persist, the strength of the Common Security and Defense Policy (CSDP) will be threatened. As we have said on more than one occasion throughout this thesis, the problem of terrorism on the Internet cannot only be addressed with military measures but requires a multidisciplinary approach. Collective defense and a unified response to terrorism is essential. Security and defense must be linked concepts and the idea of maintaining security without having a joint defensive capacity should not and cannot be conceived. The challenge of the European Union's Criminal Policy is that the threats come only from terrorism.

⁸⁵³ The Coordinated Annual Review on Defense (CARD) is included in the EU Global Strategy developed by the European Defense Agency (EDA). CARD monitors the defense plans of the Member States and helps coordinate spending and identify possible collaboration projects.

The European Union has been able to anticipate these internal dangers and in 1994 established the European Committee of the Regions.⁸⁵⁴ This Committee seeks to reduce the existing differences between the States of the Union, giving voice to the regions and cities of Europe in a consultative manner so that they evaluate a priori the impact that certain European measures may have on said regions and cities. This action not only tends to reduce differences between regions, but fundamentally to harmonize regulatory, operational or preventive policies so that they encounter less resistance in their application.

Europe should encourage this type of measures that are not aimed at establishing legal norms or criminological policies, but rather at mutual recognition of cultural identity. This institutional management model is a good example of how it can help buffer differences between regions and how to help create a more positive scenario to better accept community measures.

CONCLUSION N.º 5: THE EUROPEAN UNION'S CRIMINAL POLICY IS REACTIVE, NOT PROACTIVE.

In general terms it seems that the European Union and the Member States have become aware of the problem of international terrorism late. Naturally this is not the case, as we have stated on more than one occasion, the problem of terrorism has been a constant in European territory that forced the region to act early on this matter. The many policies, strategies, etc., that have been implemented show that for the European Union the problem of terrorism, and subsequently the phenomenon of jihadist terrorism, and jihadist terrorism on the Internet, has always been a priority.

Now, this priority has been characterized by analyzing, through expert reports, the effects of terrorist acts and their previous or derived criminal actions, and by guiding the Member States regarding the Union's priorities in this matter.

This means that the Union has focused on limiting jihadist terrorism on the Internet, but has not focused on developing a model for anticipatory analysis of possible terrorist actions on the Internet. European legislation has also acted in a similar way, and accounts for legal proposals on the problem a posteriori. Evidence of this is that there are no regulations, decisions or directives aimed at protecting, prior to the criminal act, the European digital space.

This statement does not mean in any way to propose a punishment for a criminal act that has not taken place, but rather it expresses the need to legislate in criminal matters a priori of the commission of a crime in a preventive manner.

For example, in 1969 the appearance of the Internet took place thanks to Arpanet. Almost thirty years later, approximately in 1998, the democratization of the Internet took place, which meant that the Internet became a massive and global communication channel, and in 2001 the Internet was used by jihadism to promote terrorist propaganda. Three more years had to pass from the

⁸⁵⁴ The European Committee of the Regions (CoR) represents local and regional authorities throughout the European Union. The CoR intervenes in different phases of the EU legislative process. CoR committees prepare opinions on EU legislative proposals and members meet in plenary to vote and approve these opinions. See: European Committee of the Regions. Available at: <https://cor.europa.eu/es> [Date of consultation: November 22, 2023].

massive use of the Internet to the first communication made on the network by terrorism.⁸⁵⁵ Thinking preventively would mean having “thought of the Internet”, when it emerged, as a new possible space for the criminal commission of terrorism, and then being able to instrumentalize the means to prevent the commission of crimes in the new virtual scenario. The 2001 Cybercrime Convention⁸⁵⁶ deserves a separate section. This extremely important document early marked a milestone in the observance of the Internet as a new criminal scenario. However, first, the Cybercrime Convention does not belong to the European Union, but to the Council of Europe, which would mean that this body external to the Union has been able to see, in a more proactive way than the Union itself, the future dangers of the Internet and second, it took place after the 9/11 attacks were perpetrated.

We must not forget the importance of thinking creatively about new scenarios and opportunity spaces for crime. It should not be forgotten that this same time, from 1998 to 2001, is what jihadist terrorism has had, which in this case in less than three years has taken advantage of a new communication channel and has turned it into a new crime scene. .

European cooperation for Internet surveillance and repression of its use for jihadist purposes has gradually been established in a solid and specialized way. Currently, European Criminal Policy in this area focuses on cooperation to eradicate violent content on the Internet, and this objective has become a vitally important element that integrates the current anti-terrorist fight. However, European cooperation has always taken place after the identification of completed criminal acts, and never in the face of the idea of a latent threat.

It is evident and necessary to reinforce the pillar of prevention to anticipate possible future crises that the existence of terrorism on the Internet may bring.

That is, it is urgent and essential to prepare creative multilateral and multidisciplinary approaches that allow us to anticipate threats and scenarios that have not yet occurred.

The nature of combating a threat lies in the fact of combating something not yet realized⁸⁵⁷, but it has great potential for materialization. If the current European approach is combating phenomena that are in our society, it means that the fight against terrorism is focused on eradicating situations that are already clearly established. Of course, this is necessary and logical, and in turn allows the existence of an effective Criminal Policy in meeting its objective of crime reduction. But we could promote full work that strengthens the Union's Criminal Policy, if it attempted to anticipate and prevent future actions of terrorism on the Internet, and not only focus on reducing the rate of current crimes.

Due to this reality described, we can affirm that the Criminal Policy of the European Union has traditionally tended to be reactive, and not proactive. That is, to react to the criminal acts of terrorism on the Internet, without anticipating new events.

⁸⁵⁵ It refers to the messages posted online before 9/11, in which Al Qaeda warned of an 'imminent, large-scale attack' on the United States. See: WEIMANN, Gabriel (2004), opus cit., p. 3.

⁸⁵⁶ CONSEJO DE EUROPA (2001), opus cit.

⁸⁵⁷ It does not refer in any way to early punishment, or to an advancement of the criminal barrier, but rather to the anticipation of crime scenes.

To change this usual dynamic, in 2020 the EU Security Union Strategy⁸⁵⁸ was created, which will be in force until 2025. For the first time, in an EU strategic document, priority areas in the fight against terrorism are detailed that reflect a preventive vision, because they have not yet occurred. Reference is made in the cited document to hybrid threats and the need to increase the resilience of the Union's critical infrastructures, because it is estimated that jihadist terrorism on the Internet will move from cybercrime to cyberwar.

However, this category change from cybercrime to cyberwar, defined by future systematic attacks on EU infrastructure and by bioterrorism⁸⁵⁹, was proposed by the United States in 2017⁸⁶⁰, which means that Europe's Criminal Policy needs to be justified by current criminal acts or legitimized by the US.

It is necessary to continue researching future trends in the extreme radicalization of jihadism and evaluate not only the criminal practices and threats of terrorism present on the Internet, but also the probable and future ones for preventive and proactive intervention.

⁸⁵⁸ COMISIÓN EUROPEA (2020), opus cit.

⁸⁵⁹ Terrorism committed through weapons of mass destruction of a chemical, biological, radiological and nuclear nature, the planning, coordination and execution of which can be committed through computer systems and remotely.

⁸⁶⁰ UNITED NATIONS OFFICE OF COUNTER-TERRORISM (2017): *Ensuring Effective Interagency Interoperability and Coordinated Communication in Case of Chemical and/or Biological Attacks*. New York: United Nations Headquarters.

BIBLIOGRAFÍA

FUENTES BIBLIOGRÁFICAS

ABAD CASTELOS, Monserrat (2012): «El concepto jurídico del terrorismo y los problemas relativos a su ausencia en el ámbito de las Naciones Unidas», en: CONDE PÉREZ, Elena (Dir.) /IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, pp. 105-123.

AGUIRRE ROMERO, Joaquín M. (2004): «Ciberspacio y comunicación: nuevas formas de vertebración social en el Siglo XXI», *Espéculo. Revista de estudios literarios (EREL)*, Universidad Complutense de Madrid, N.º 27, jul-oct.

ALONSO MARCOS, Antonio (2011): «Hizb ut Tahrir en el Líbano: Sus aportaciones al islam político», *Revista CIDOB d'Afers Internacionals*, núm. 93-94, p. 201-217.

ALTHEIDE, David L. (1996): *Qualitative media analysis*. Thousand Oaks: Sage.

ALTHEIDE, David L. (2006): *Terrorism and the Politics of Fear*. Lanham: Rowman & Littlefield Publishers.

ANDERSON, David Q.C. (2017): *Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 And Police. Internal Reviews*, Unclassified, December 2017, London.

ANDRADE, Luis Julio/AYUNTAMIENTO DE MÁLAGA (2017): *I Plan Transversal por la Convivencia y la Prevención de la Radicalización Violenta en la Ciudad de Málaga 2017-2020, elaborado por el Excmo. Ayuntamiento de Málaga y la Universidad de Málaga*.

AYALA PÉREZ, Teresa (2012): «Marshall McLuhan, las redes sociales y la Aldea Global», *Revista Educación y Tecnología*, N.º 2, pp. 8-20.

BANCO INTERAMERICANO DE DESARROLLO (BID)/ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA) (2020): *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*.

BARATTA, Alessandro (1997): «Política Criminal: Entre la política de seguridad y la política social», en: CARRANZA, Elías (Coord.), *Delito y Seguridad de los Habitantes*, México, D.F.: Siglo XXI, pp. 80-95.

BECERRA MUÑOZ, José (2013): *La toma de decisiones en Política criminal. Bases para un análisis multidisciplinar*. Valencia: Tirant Lo Blanch.

BECKER, Gary S. (1968) «Crime and Punishment: An Economic Approach», *Journal of Political Economy*, University of Chicago Press, Vol. 76, No. 2, pp. 169-217.

BOTTA, Paulo (2007): *El concepto de “Fundamentalismo Islámico”*. Buenos Aires: Centro de Estudios del Medio Oriente Contemporáneo (Cemoc).

BOUCHARD, Martin (2015): *Social Networks, Terrorism and Counter-terrorism Radical and Connected*. London: Routledge

BOWYER BELL, John (1978): *A time of terror*. New York: Basic Books.

CABINET OFFICE (2008): *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, March 2008, Cm 7291, London.

CALDUCH CERVERA, Rafael (2007): «Conflictos internacionales culturales y violencia terrorista», *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, pp. 23-80.

CANCELO SANMARTÍN, Mercedes (2017): *La comunicación en las fuerzas de seguridad*. Barcelona: UOC.

CANCIO MELIÁ, Manuel (2009): «Sentido y límites de los delitos de terrorismo en Derecho penal contemporáneo», *Revista Internacional*, N.º 26, pp. 47-84.

CANO PAÑOS, Miguel Ángel (2008a): «Internet y terrorismo islamista. Aspectos criminológicos y legales», *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, diciembre (22), pp. 67-88.

CANO PAÑOS, Miguel Ángel (2008b): «Los inicios de la lucha antiterrorista en Alemania. Análisis de la legislación penal y procesal en las décadas de 1970-1980», *Revista Electrónica de Ciencia Penal y Criminología* (en línea), núm. 10-14, pp. 1-31.

CANO PAÑOS, Miguel Ángel (2008c): «Respuestas legales al terrorismo yihadista. El ejemplo de Alemania», *Athena Intelligence Journal*, Vol. 3, N.º 1, pp. 45-77.

CANO PAÑOS, Miguel Ángel (2010a): «El Derecho penal ante los desafíos del terrorismo global», *Indret: Revista para el Análisis del Derecho*, N.º 3, pp. 1-32.

CANO PAÑOS, Miguel Ángel (2010b): «Reflexiones en torno al “viejo” y al “nuevo” terrorismo», *Revista Española de Investigación Criminológica (REIC)*, Artículo 7, Número 7, pp. 21-56.

CANO PAÑOS, Miguel Ángel (2011): «Reflexiones y experiencias desde las entrañas del yihadismo militante. Análisis de la autobiografía de Eric Breininger», *UNISCI Discussion Papers*, (26), mayo de 2011, pp. 191-223.

CANO PAÑOS, Miguel Ángel (2015): «El binomio Internet/Terrorismo islamista. De una amenaza virtual a un peligro real. Una visión desde la Criminología y el Derecho penal», *presentación de Power Point*, Doctorado en la Universidad de Granada.

CANO PAÑOS, Miguel Ángel (2016): «Odio e incitación a la violencia en el contexto del terrorismo islamista. Internet como elemento ambiental», *Revista para el análisis del derecho In Dret*, 4/2016, pp. 1-37.

CANO PAÑOS, Miguel Ángel (2018): «La lucha contra la amenaza yihadista más allá del Derecho penal. Análisis de los programas de prevención de la radicalización y desradicalización a nivel europeo», *Revista de Estudios en Seguridad Internacional (RESI)*, Vol. 4 Núm. 2 (2018), pp. 177-205.

CANO PAÑOS, Miguel Ángel (2019a): «Criminalidad virtual: ¿Vino viejo en botellas nuevas? Traducción y nota previa de Miguel Ángel Cano Paños», *Revista Electrónica de Criminología*, 02-01, 1-8, pp. 1-8.

CANO PAÑOS, Miguel Ángel (2019b): «La violencia terrorista como espectáculo en Internet. Una aproximación criminológica», *Revista Científica General José María Córdova*, 17(28), 2019, pp. 691-717.

CANO PAÑOS, Miguel Ángel (2019c): «La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico», *Revista Científica General José María Córdova*, 17(26), 2019, pp. 271-287.

CAPRON, Timothy A./MIZRAHI, Stephanie Bernice (2016): *Terrorism and Homeland Security*. New York: Sage.

CARRANZA, Elías (2007): «La política criminológica integral de las Naciones Unidas», en: Congreso Nacional de Criminología”, Facultad de Derecho de la Universidad de Buenos Aires, Argentina.

CARRASCO ANDRINO, María del Mar (2019): «Derechos fundamentales y legislación antiterrorista: ¿Qué hemos perdido en el camino?», *Estudios penales y criminológicos*, vol. XXXIX, pp. 59-105.

CARRILO DURÁN, María Victoria (2014): «La comunicación estratégica y sus profesionales», *Revista Mediterránea de Comunicación*, vol. 5, N.º 2, pp. 22-46.

CARTHY, Sara (2021): *Lessons Learned from Alternative Narrative Campaigns*, RAN External Expert, European Commission, pp. 1-20.

CASTELLS, Manuel (2000): *La era de la información: economía, sociedad y cultura. Volumen I: La Sociedad Red*. Madrid: Alianza Editorial.

CASTELLS, Manuel (2009): *Comunicación y poder*. Madrid: Alianza Editorial.

CEBADA ROMERO, Alicia (2008): *La Unión Europea: ¿una acción exterior inteligente?*, Madrid: Iustel.

CENTRO CRIPTOLÓGICO NACIONAL. CNI (2019): IA-13/19. Ciberamenazas y tendencias 2019. CNN_CERT Resumen Ejecutivo.

CHARMELOT, Jacques (2009): «Le Smart Power Américain, un défi pour l'Europe», *Questions d'Europe*, N.º 127.

CHAVES-MONTERO, Alfonso (2018): «La utilización de una metodología mixta en investigación social», en: DELGADO SANTA GADEA, Kenneth/GADEA, Walter Federico/VERA-QUÍÑONEZ, Sara. (Coords.), *Rompiendo barreras en la investigación*, Machala: UTMACH, pp. 164-184.

CHOMSKY, Noam/HERMAN, Edward, S. (2000): *Los guardianes de la libertad: propaganda, desinformación y consenso en los medios de comunicación de masas*. Barcelona: Crítica.

CLUB OF VENICE (2017): *Convergences N° 10: Public Communication in Europe*, pp. 1-136.

COHEN, Bernard Cecil (1963): *The Press and Foreign Policy*. Princeton: Princeton University Press.

COMISIÓN EUROPEA (2020): *Estrategia de la UE para una Unión de la Seguridad: integrar las medidas individuales en un nuevo ecosistema de seguridad*. Bruselas, 24 de julio de 2020.

COMISIÓN EUROPEA (2021): *Comunicado de Prensa. La Comisión propone ampliar la lista de «delitos de la UE» a la incitación al odio y a los delitos motivados por el odio*, 9 de diciembre de 2021.

COMISIÓN EUROPEA (2022): *Comunicado de Prensa. Ley de Servicios Digitales: entran en vigor las normas determinantes de la UE para las plataformas en línea*, 16 de noviembre de 2022.

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO (2016): *Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea*, (JOIN/2016/018 final).

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES (2013): *Prevenir la radicalización hacia el terrorismo y el extremismo violento: una respuesta más firme de la UE*, (COM/2013/941 final).

COMUNICACIÓN UE: *Apoyo a la prevención y radicalización que conduce al extremismo violento* (COM/2016/379 final).

COMUNICACIÓN UE: *Estado de la aplicación de las medidas que figuran en la comunicación de la Comisión sobre apoyo a la prevención de la radicalización que conduce al extremismo violento*, (COM/2016/379 final).

CONSEJO DE LA UNIÓN EUROPEA (2003): *Estrategia Europea de Seguridad (EES, 2003): Una Europa segura en un mundo mejor*, Bruselas.

CONSEJO DE LA UNIÓN EUROPEA (2010): Proyecto de Estrategia de Seguridad Interior de la Unión Europea: "Hacia un modelo europeo de seguridad" 7120/10 JAI 182.

CONSEJO EUROPEO (2010a): *Estrategia de Seguridad Interior de la Unión Europea. Hacia un modelo europeo de seguridad*. Luxemburgo: Oficina de publicaciones de la Unión Europea.

COUNCIL DECISION (2017): CFSP 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

COUNCIL OF THE EUROPEAN UNION (2016): A Global Strategy for the European Union's Foreign and Security Policy. 14392/16, Brussels, 14 November 2016.

DE CASTRO RUANO, José Luis (2015): «La evolución de la Unión Europea como actor en materia de seguridad y defensa. En busca de un relanzamiento siempre pendiente», *Cuadernos Europeos de Deusto*, Universidad de Deusto, Número Especial 01, pp. 19-48.

DE LA CORTE IBÁÑEZ, Luis (2012): «El terrorismo yihadista internacional a principios del siglo XXI», en: CONDE PÉREZ, Elena (Dir.) /IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, pp. 27-42.

DE LA CORTE IBÁÑEZ, Luis (2013): «¿Hasta qué punto convergen el terrorismo global y la criminalidad organizada? Parámetros generales y escenarios críticos», *Revista del Instituto Español de Estudios Estratégicos*, (1), pp. 149-176.

DE LA VEGA, Julio Cesar (1988). *Diccionario consultor político* [verde]. Buenos Aires: Librograf editora.

DESAI, Meghnad (2007): *Rethinking Islamism*. Londres: I.B. Tauris.

DIARIO LA LEY (2015): Comentario a la LO 2/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. (BOE 31 de marzo de 2015), Sección documento online, N.º 8511, Editorial La Ley.

DIAZ, Gustavo (2007): «La cooperación entre servicios de inteligencia en el marco de la Unión Europea: ¿cooperación transnacional o multinacional?», *UNISCI Discussion Papers*, No 13, pp. 43-51

DÍEZ RIPOLLES, José Luis (2004): «El nuevo modelo penal de la seguridad ciudadana», *Revista electrónica de ciencia penal y criminología (RECPC)*, 06-03, pp. 1-34.

DÍEZ RIPOLLES, José Luis (2005): «De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado», *Revista Electrónica de Ciencia Penal y Criminología*, N.º 7, pp. 1-37.

DUNLAP, Charles J. Jr. (2001): «Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts», *Working Paper*, Carr Center for Human Rights, John F. Kennedy, Harvard.

ENTMAN, Robert M. (2007): «Framing Bias: Media in the Distribution of Power», *Journal of Communication*, 57, pp. 163-173.

ESER, Albin (2004): «Consideración final», GOMEZ RIVERO, Carmen (Trad.), en: ESER, Albin/HASSEMER, Winfried/BURKHARDT, Björn (Coords.) /MUÑOZ CONDE, Francisco (Coord. versión española), *La ciencia del Derecho penal ante el cambio de milenio*, Valencia: Tirant lo Blanch, pp. 463-476.

ESTRATEGIA DE LA UNIÓN EUROPEA DE LUCHA CONTRA EL TERRORISMO (14469/4/05).

ESTRATEGIA NACIONAL CONTRA EL TERRORISMO (2019): Ministerio del Interior y Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). Aprobado por el Consejo de Seguridad Nacional según orden PCI/179/2019, de 22 de febrero.

EUCPN (2019): *European Crime Prevention Monitor 2019/1: Radicalisation and violent extremism*. Brussels: European Crime Prevention Network.

EUROJUST (2007): *Informe anual 2007*, de enero de 2008.

EUROPEAN COMMISSION (2017): *The contribution of youth work to preventing marginalisation and violent radicalisation. A practical toolbox for youth workers & Recommendations for policy makers*, Results of the expert group set up under the European Union Work Plan for Youth for 2016-2018, Luxembourg: Publications Office of the European Union, pp. 1-50.

EUROPEAN COMMISSION. JOINT RESEARCH CENTRE (2022): *Security by Design: Protection of public spaces from terrorist attacks*. Luxembourg: Publications Office of the European Union.

EUROPEAN COMMISSION'S EXPERT GROUP ON VIOLENT RADICALISATION (2008): *Radicalisation processes leading to acts of terrorism* (Report), Brussels: European Commission.

EUROPEAN COUNCIL (2004): *Headline Goal 2010*. Approved by General Affairs and External Relations Council on 17 May 2004 endorsed by the European Council of 17 and 18 June 2004.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (2015): ENISA Threat Landscape 2015, January 2016.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (2023): *ENISA Threat Landscape 2023*, October 2023

EUROPOL (2021): *Internet Organised Crime Threat Assessment (IOCTA) 2021*, Publications Office of the European Union.

FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY. FEDERAL GOVERNMENT (2023): *Report of the Independent Expert Group on Anti-Muslim Sentiment*, August 2023, Berlin, pp. 1-370.

FELIP I SABORIT, David. (2010): «Observaciones a La Expansión diez años después», en: ROBLES PLANAS, Ricardo y SANCHEZ-ORTIZ GUTIERREZ, Pablo (Coords.), *La crisis del Derecho penal contemporáneo*, vol. 21, Barcelona, Atelier, pp. 65-88.

FELSON, Marcus/BOBA, Rachel (2009): *Crime and everyday life*. Newcastle: Sage Group.

FELSON, Marcus/CLARKE, Ronald (1998): «Opportunity makes the thief. Practical theory for crime prevention», *Research, Development and Statistics*, Police Research Series Paper N° 98, London.

FERNÁNDEZ CARDOSO, S. (2011). «Teoría, sociedad y poder en Talcott Parsons, C. Wright Mills, Jurgen Habermas y Anthony Giddens», Tesis de Doctorado, Universidad Católica Argentina, Facultad de Ciencias Sociales, Políticas y de la Comunicación, Buenos Aires: UCA.

FERNÁNDEZ LIESA, Carlos R. (2018): «Sujetos de Derecho y actores no estatales: cuestiones de Derecho internacional», *Anuario español de derecho internacional*, N.º 34, pp. 87-113.

FERRERO, Guglielmo (1998): *Poder. Los genios invisibles de la ciudad*. Madrid: Tecnos.

FUENTES I GASÓ, Josep Ramon (2017): «El régimen jurídico de prevención de peligros en Alemania: La vigencia de un modelo histórico», *Revista Aragonesa de Administración Pública*, núm. 49-50, Zaragoza, pp. 26-86.

GADEA ALDAVE, Gilda (2014): «Delito y propaganda terrorista en Internet», en: RODRÍGUEZ TERCEÑO, José/FERNÁNDEZ PARADAS, Antonio (Coords.), *Nuevas culturas y sus lecturas*, Madrid: McGraw Hill, pp. 245-259.

GARCÍA GURRIONERO, Mario (2013): *El papel del terror en la sociedad*, Madrid: Maia.

GARCÍA LÓPEZ, Miguel Angel/ PAŠIĆ, Lana (2018): *Youth work against violent radicalisation. Theory, concepts and primary prevention in practice*, Council of Europe and European Commission, April 2018, pp. 1-82.

GOLDSTEIN, Brooke M./MEYER, Aaron E. (2009): «"Legal Jihad": How Islamist Lawfare Tactics Are targeting Free Speech», *ILSA Journal of International & Comparative Law*, Vol 15:2, pp. 395-410.

GONZÁLEZ COLLANTES, Talía (2014): «Los ficheros de internos de especial seguimiento: un ejemplo de la penetración de la cultura de emergencia y la excepcionalidad en el ámbito penitenciario», *Revista Pensamiento Penal*, 11 de agosto, Asociación Pensamiento Penal, pp.1-16.

GONZÁLEZ GUARDA, Claudio (2017): «La Política Criminal aplicada (PCA): La deriva de la Política Criminal hacia la política pública», *Nuevo Foro Penal*, No. 88, enero-junio, Universidad EAFIT, pp. 185-216.

HABERMAS, Jürgen (1998): *Facticidad y validez*, Madrid: Trotta.

HAYES, Ben/ QURESHI, Asim (2016): *We Are Completely Independent. The Home Office, Breakthrough Media and the Prevent Counter Narrative Industry*, Report, London: CAGE.

HECKER, Marc (2021): *Once a Jihadist, Always a Jihadist? A Deradicalization Program Seen from the Inside*, Focus stratégique, N° 102 bis, Ifri, February 2021, pp. 1-78.

HM GOVERNMENT (2009): *The National Security Strategy of the United Kingdom: Security for the Next Generation*, June 2009, Cm 7590, London.

HM GOVERNMENT (2010): *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010, Cm 7953, London.

HM GOVERNMENT (2011a): *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, July 2011, Cm 8123, London.

HM GOVERNMENT (2011b): *Prevent Strategy*, June 2011, Cm 8092, London.

HM GOVERNMENT (2012): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report*, March 2013, Cm 8583, London.

HM GOVERNMENT (2013): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report*, April 2014, Cm 8848, London.

HM GOVERNMENT (2014): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2014*, March 2015, Cm 9048, London.

HM GOVERNMENT (2015a): *CONTEST The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2015*, July 2016, Cm 9310, London.

HM GOVERNMENT (2015b): *National Security Strategy and Strategic Defence and Security Review, A Secure and Prosperous United Kingdom*, November 2015, Cm 9161, London.

HM GOVERNMENT (2016): *National Cyber Security Strategy 2016-2021*, London.

HM GOVERNMENT (2018): *The United Kingdom's Strategy for Countering Terrorism*, June 2018, Cm 9608, London.

HM GOVERNMENT (2022a): *Government Cyber Security Strategy 2022-2030: Building a cyber resilient public sector*, London.

HM GOVERNMENT (2022b): *Ciberestrategia Nacional 2022: Lideramos el ciberfuturo con la participación activa de la totalidad del RU*, London.

HM GOVERNMENT (2023): *The United Kingdom's Strategy for Countering Terrorism*, July 2023, CP 903, London.

HUERTAS DÍAZ, Omar (2009): «Durkheim: la perspectiva funcionalista del delito en la criminología», *Revista Criminalidad Policía Nacional DIJIN*, Bogotá, D. C., vol. 51, núm. 2, dic, pp. 103-115.

INSTITUTE FOR ECONOMICS & PEACE (2018): *Global Terrorism Report 2018: Measuring and understating the impact of terrorism*, Sydney, November 2018.

JAKOBS, Günther (2004): «La ciencia penal ante los retos del futuro», MANSO, Teresa (Trad.), en: ESER, Albin/HASSEMER, Winfried/BURKHARDT, Björn (Coords.) /MUÑOZ CONDE, Francisco (Coord. versión española), *La ciencia del Derecho penal ante el cambio de milenio*, Valencia: Tirant lo Blanch, pp. 53-63.

JEFFREY, Ian Ross (2006): *Political Terrorism: An Interdisciplinary Approach*, New York: Peter Lang Publishing.

JIMÉNEZ CHAVES, Viviana Elizabeth/COMET WEILER, Cornelio (2016): «Los estudios de casos como enfoque metodológico», *ACADEMO Revista De Investigación En Ciencias Sociales Y Humanidades*, 3(2).

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL
The EU's Cybersecurity Strategy for the Digital Decade.

JORDÁN, Javier/TORRES SORIANO, Manuel R. (2007): «Internet y actividades terroristas: el caso del 11-M», *Revista Profesional de la información*, (2)16, marzo de 2007, pp. 123-130.

JUERGENSMEYER, Mark (2022): «Othering in ISIS», en: JUERGENSMEYER, Mark (Ed.)/MOORE, Kathleen (Ed.)/ SACHSENMAIER, Dominic (Ed.), *Religious Othering: Global Dimensions*, London: Routledge, pp. 111-122.

KARSTEDT, Susanne (2002): «Durkheim, Tarde and beyond», en: *Criminology and Criminal Justice*, 2(2), (111-123).

KOEHLER, Daniel (2021): «La desradicalización en Alemania: prevenir y combatir el extremismo violento», *Revista CIDOB d'Afers Internacionals*, N.º 128, pp. 59-79.

LABORATORIO DE INVESTIGACIÓN ESET (2021): *ESET Security Report (ESR) Latinoamérica 2021*.

LAHNAIT, Fatima (2021): «Prevenir el extremismo violento para combatir el yihadismo autóctono: aprender de la experiencia», *Revista de Ciencias Sociales Iconos* 71, vol. XXV, N.º 71, septiembre-diciembre 20, FLACSO, Ecuador, pp. 43-57.

LEJINS, Peter (1967): «The field of prevention», en: AMOS, William E./WELLFORD, Charles F. (Eds.), *Delinquency prevention: Theory and practice*, Englewood Cliffs: Prentice-Hall.

LESACA, Javier (2017): *Armas de seducción masiva*, Barcelona: Ediciones península.

LÓPEZ PEREGRÍN, Carmen. (2003): «¿Lucha contra la criminalidad mediante el cumplimiento íntegro y efectivo de las penas?», *Revista Española de Investigación Criminológica*, N.º 1, pp. 7-11.

MARÍN DUEÑAS, Pedro Pablo/LASSO DE LA VEGA GONZÁLEZ, María del Carmen (2017): «La efectividad de las páginas web en la comunicación empresarial de las pequeñas y medianas empresas. Un estudio en PYMES de la provincia de Cádiz», *ZER: Revista de Estudios de Comunicación = Komunikazio Ikasketen Aldizkaria*, 22(42).

MARRERO ROCHA, Inmaculada (2022): «La prevención de la radicalización violenta de corte yihadista en la Unión Europea», en: *Revista de Derecho Comunitario Europeo*, 73, pp. 793-828.

MCCOMBS, Maxwell E. y SHAW, Donald (1972): «The Public Opinion Quarterly», *Oxford University Press*, Vol. 36, No. 2, pp. 176-187.

MEDINA ARISA, Juanjo (2010): «Políticas de seguridad ciudadana en el contexto urbano y prevención comunitaria. La experiencia anglosajona», en: *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 12-02, pp. 1-36.

MESTRE DELGADO, Esteban (1987): *Delincuencia terrorista y Audiencia Nacional*. Madrid: Centro de publicaciones del Ministerio de Justicia.

MIETTINEN, Samuli (2013): *Criminal Law and Policy in the European Union*. London: Routledge.

MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA (2015): *Plan Estratégico Nacional de Lucha contra la Radicalización Violenta* (PEN-LCRV), de 30 de enero.

MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA (2020): *Informe sobre la Cibercriminalidad en España 2020*.

MINISTRY OF JUSTICE (2023): *Cyber Security Strategy 2023-2028*, London.

MIRAVITLLAS POUS, Enric (2015): «Hacia una tipología de contranarrativas frente al extremismo violento», en: *Actas de XII Congreso de la Asociación Española de Ciencia Política y de la Administración*, organizado por AECPA, celebrado en Euskal Herriko Unibertsitatea, Universidad del País Vasco, San Sebastián, 13 a 15 de julio de 2015, pp. 1-21.

MIRÓ LLINARES, Fernando (2011): «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», *Revista Electrónica de Ciencia Penal y Criminología (RECPC)*, pp.1-55.

MOGHADDAM, Fathali M. (2009): «De-Radicalization and the Staircase from Terrorism», en CANTER, David (Ed.), *The Faces of Terrorism: Multidisciplinary Perspectives*, New Jersey: Wiley, pp. 277-292.

MONTANER PERALTA, Gonzalo (2020): *Están con nosotros o con los terroristas*. Santiago: Ariadna Ediciones.

MORA BENAVENTE, Enrique (2010): «Introducción. La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa», *Cuadernos de Estrategia*, N.º 145, Marzo 2010, Instituto Español de Estudios Estratégicos. Ministerio de Defensa de España.

MORALES ANTONIAZZI, Mariela (2023), «Protección y garantías transnacionales para nuevos y viejos derechos», en: ARAGÓN REYES, Manuel/VALADÉS RÍOS, Diego/TUDELA ARANDA, José, *Derecho Constitucional del Siglo XXI: desafíos y oportunidades*, pp. 129-167.

MORGENTHAU, Hans J. (2020): *Política entre las naciones. La lucha por el poder y la paz*, Santiago de Chile: Ediciones Jurídicas Olejnik.

MOTLEY, James B. (1985): «Terrorist Warfare: Formidable Challenges», *The Fletcher Forum*, vol. 9, N° 2, pp. 295–306.

MOYANO PACHECO, Manuel/TRUJILLO MENDOZA, Humberto Manuel (2013): *Radicalización Islamista y Terrorismo. Claves psicosociales*. Granada: UGR-MADOC.

MUÑOZ CONDE, Francisco (2011): «La generalización del Derecho penal de excepción: tendencias legislativas y doctrinales: entre la tolerancia cero y el Derecho penal del enemigo», *Ciencia Jurídica*, División de Derecho, Política y Gobierno, Universidad de Guanajuato, año 1, N.º 1, pp. 113-142.

NYE, Joseph. (2004): *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

OBSERVATORIO DE POLÍTICA CRIMINAL (2015): *¿Qué es la política criminal?*, Dirección de Política Criminal y Penitenciaria, Ministerio de Justicia y del Derecho de Bogotá, Bogotá, D.C., DC-001/2015.

OÑATE RUBALCABA, Pablo (2005): «Participación política, partidos y nuevos movimientos sociales», *Revista mexicana de ciencias políticas y sociales*, N.º 194, pp. 103-136.

ORTA MARTÍNEZ, Raymond (2005): «Ciberterrorismo», *Alfa Redi, Derecho y Nuevas Tecnologías* (82).

ORTIZ LOBO, Alberto (2019): «Contra la prevención sanitaria individual del sufrimiento mental», *Revista de la Asociación Española de Neuropsiquiatría*, vol.39 no.135, ene./jun. 2019, pp. 177-191.

PANORAMA DE EUROPOL (2012): *Informe general sobre las actividades de Europol*, de 7 de mayo de 2012, (1423-74r2).

PEGORARO, Juan (2001): «Derecha criminológica, neoliberalismo y política penal», *Delito y Sociedad*, 15/16, pp. 141-160.

PÉREZ BERNÁRDEZ, Carmela (2012): «La difícil coordinación de la política antiterrorista de la Unión Europea», en: CONDE PÉREZ, Elena (Dir.) /IGLESIAS SÁNCHEZ, Sara (Coord.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, pp. 127-157.

PÉREZ MACHÍO, Ana I. (2008): «Normativa internacional para la erradicación de todas las formas de terrorismo», en: DE LA CUESTA, José Luis/MUÑAGORRI, Ignacio (Dir.), *Aplicación de la normativa antiterrorista*, Donostia: IVAC/KREI, pp. 152-166.

PROCTOR, Natalia (2019): «Anti-Radicalisation. Report 2019», *Counter Terrorism Preparedness Network (CTPN)*, First edition, London Resilience Group, pp. 1-54.

PUENTE GUERRERO, Patricia (2011): «La regulación de los delitos de terrorismo en la L.O. 5/2010. ¿Son los terroristas nuestros “enemigos”? Especial referencia a la libertad vigilada», *Derecho penal y Criminología*, Vol. 32, No. 93, julio-diciembre, pp. 83-119.

RADICAL ONLINE EDUCATION (2017): *How to prevent radicalization*, Digital guide, Project Co-funded by the Erasmus+, Programme of the European Union, October 2017 to March 2019, Danish Youth Team (Denmark), Projuven (Spain), OEJAB (Austria), Alternativi International (Bulgaria), by Danish National Agency for Higher Education.

RAMOS TAPIA, María Inmaculada (2013): «Delitos de abusos sexuales a menores: arts. 182, 183 y 183 bis)», en: ÁLVAREZ GARCÍA, Francisco Javier (Dir.) /DOPICO GÓMEZ-ALLER, Jacobo (Ed.), *Estudio crítico sobre el Anteproyecto de reforma penal de 2012*, Valencia: Tirant lo Blanch, pp. 659-668.

RAMOS TAPIA, María Inmaculada (2015): «La tipificación de los abusos sexuales a menores: el proyecto de reforma de 2013 y su adecuación a la Directiva 2011/92/UE», en: VILLACAMPA ESTIARTE, Carolina/AGUADO-CORREA, Teresa (Coords.), *Delitos contra la libertad e indemnidad sexual de los menores*, Aranzadi, Pamplona, 2015, pp. 107-137.

REINARES, Fernando (2005): «Conceptualizando el terrorismo internacional», *Análisis del Real Instituto Elcano*, (24), Madrid: Real Instituto Elcano, pp. 4-7.

REINARES NESTARES, Fernando/ JAIME-JIMÉNEZ, Oscar (2000): «Countering terrorism in a new democracy: the case of Spain», en: REINARES NESTARES, Fernando (Ed.), *European democracies against terrorism: governmental policies and intergovernmental cooperation*, Ashgate, pp. 119-145.

RODRÍGUEZ-SERRANO, Aarón (2017): «Narrativa audiovisual, ontología y terrorismo: paradojas comunicativas en los videos del Estado Islámico», *Palabra Clave*, 20 (1), pp. 96-115.

RUIZ DÍAZ, Lucas J. (2017): «La prevención de la radicalización en la estrategia contra el terrorismo de la Unión Europea. Entre Soft Law e impulso de medidas de apoyo», *REDI*, vol. 69, 2, pp. 257-280.

SÁDABA, Teresa. (2008): *Framing: El encuadre de las noticias. El binomio terrorismo-medios*, Buenos Aires: La Crujía.

SAID, Behnam T./FOUAD, Hazim (2018): «Countering Islamist Radicalisation in Germany: A Guide to Germany's Growing Prevention Infrastructure», *ICCT Policy Brief*, September, International Centre for Counter-Terrorism-The Hague, pp. 1-17.

SÁNCHEZ-OSTIZ, Pablo (2012): *Fundamentos de Política Criminal. Un retorno a los principios*. Madrid: Marcial Pons.

SANZ MULAS, Nieves (2019): *Política Criminal*. Managua: INEJ.

SCHMID, Alex P. (2004): «Estadísticas sobre el terrorismo: Dificultades de medir las tendencias del terrorismo mundial», en: SCHMID, Alex P. (Ed.), *Foro sobre el delito y la sociedad*, Vol. 4, N.º 1 y 2, New York: UNODC, pp. 55-78.

SCHMID, Alex P. (2004): «Terrorism. The definitional problem», *Reserve Journal of International Law*, 36(2), pp. 375-420.

SCHMID, Alex. P./JONGMAN, Albert. J. (2005); *Political Terrorism: A new guide to actors. Authors, concepts, data bases, theories, and literature*, New Brunswick: Transaction Publishers.

SILVA SÁNCHEZ, Jesús María (2001): *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, Madrid: Civitas.

SIMÓN, Luis/GARCÍA ENCINA, Carlota (2022): «La nueva Estrategia de Seguridad Nacional de EEUU», *Real Instituto Elcano ARI 69/2022*, 8 de noviembre de 2011, pp. 1-9.

SOZZO, Máximo (2000): «¿Hacia la Superación de la Táctica de la Sospecha? Notas sobre Prevención del Delito e Institución Policial», en: *Centro de Estudios Legales y Sociales*, Buenos Aires: CELS, pp. 1-61.

THE INTERPARLIAMENTARY EUROPEAN SECURITY AND DEFENCE ASSEMBLY (2003): Assembly of Western European Union. *Recommendation 726, on the United States National Security Strategy and its consequences for European defence*, adopted unanimously by the Assembly without amendment on 4 June 2003 (4th sitting).

THE WHITE HOUSE (2002): *The National Security Strategy of the United States of America*. Washington, September 2002.

TOBOSO BUEZO, Mario (2016): «Una aproximación a la contranarrativa yihadista», *Grupo de Estudios de Seguridad Internacional, GESI*, Universidad de Granada, pp. 1-18.

TORRES DEL MORAL, Antonio (2014): «Seguridad y Estado de Derecho», en CASTRO-RIAL GARRONE, Fanny (Coord.), *Contribución de la Guardia Civil a la seguridad*, pp. 35-52.

TORRES SORIANO, Manuel R. (2007): *La dimensión propagandística del terrorismo yihadista global*. Tesis doctoral. Granada: Universidad de Granada.

TORRES SORIANO, Manuel (2015): «¿Es el yihadismo una ciber- amenaza?», *Revista de Occidente*, no 406, marzo 2015, pp. 1-11.

TORRES SORIANO, Manuel (2016): «Tendencias en procesos de radicalización», en: *Cuadernos del Centro Memorial de las víctimas del terrorismo. Terrorismo internacional: análisis de la radicalización y estrategias de prevención*, N.º 2, diciembre 2026, pp. 95-110.

TRACHTMAN, Joel P. (2016): «Integrating Lawfare and Warfare», *Boston College International and Comparative Law Review* 39, Nº 2, pp. 267-281.

TRIBUNAL DE CUENTAS EUROPEO (2018): «Hacer frente a la radicalización que conduce al terrorismo: la Comisión respondió a las necesidades de los Estados Miembros, pero con algunas deficiencias en la coordinación y la evaluación», Informe Especial N.º 13, pp. 1-37.

UNIDAD DE REFERENCIA DE INTERNET (2019): Informe de actividad 2019 de la Unidad de Referencia de Internet de la Unión Europea, Europol, 25 de octubre 2020.

UNITED NATIONS OFFICE OF COUNTER-TERRORISM (2017): *Ensuring Effective Interagency Interoperability and Coordinated Communication in Case of Chemical and/or Biological Attacks*. New York: United Nations Headquarters.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (2012): *The use of the Internet for terrorist purposes*. New York: UNODC.

US DEPARTMENT OF DEFENSE (2022): *2022 National Defense Strategy of the United States of America, including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*, Washington DC, 27/X/2022.

VALLS PRIETO, Javier/MORILLAS CUEVA, Lorenzo (2006): «Hacia la nueva realidad de un Derecho penal europeo», *Revista de la Facultad de Derecho de la Universidad de Granada*, núm. 9, p. 159-184.

VERES CORTÉS, Luis (2005): «La simbiosis del terrorismo con los medios de comunicación», en *Información para la paz: autocritica de los medios y responsabilidad del público*. Actas del Congreso Internacional de Ética y Derecho de la Información organizado por la Universidad CEU Cardenal Herrera, pp. 587-594.

VIRGINIA DEPARTMENT OF CRIMINAL JUSTICE SERVICES (2018): *Crime Prevention History and Theory*, Course, Day 1 Session 2, DCJS, pp. 1-69.

WATERS, Melissa A. (2010): «'Lawfare' in the War on Terrorism: A Reclamation Project», *Case Western Reserve Journal of International Law*, Volume 43, Issue 1, pp. 327-334.

WEBER, Max (1967): *El político y el científico*, Madrid: Alianza.

WEIMANN, Gabriel (2004): «Terrorismo e internet», *Revista Ética Net*, (3), pp. 1-6.

WEINBERG, Leonard/PEDAHZUR, Ami/HIRSCH-HOEFLER, Sivan (2004), «The Challenges of Conceptualizing Terrorism», *Terrorism and Political Violence*, 16(4), pp. 777-794.

WHITTAKER, David. J. (2003): *The Terrorism Reader*, London: Routledge.

FUENTES ELECTRÓNICAS Y SITIOS WEBS

«70 años de defensa colectiva», Ejército de Tierra, Ministerio de Defensa, Gobierno de España, Disponible en: https://ejercito.defensa.gob.es/gl/reportajes/2019/82_aniversario_otan.html [Fecha de consulta: 06 de noviembre de 2023].

«About Us – Global Engagement Center», *US Department of State*. Disponible en: <https://www.state.gov/about-us-global-engagement-center-2/> [Fecha de consulta: 29 de noviembre de 2023].

Action Counters Terrorism (ACT). Disponible en: <https://act.campaign.gov.uk> [Fecha de consulta: 29 de diciembre de 2023].

Agencia de la Unión Europea para la Ciberseguridad. Disponible en: <https://www.enisa.europa.eu/about-enisa/about/es> [Fecha de consulta: 22 de noviembre de 2023].

Agencia Europea de Defensa (EDA). Disponible en: [https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-\(card\)](https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)) [Fecha de consulta: 03 de noviembre de 2023].

AKRAN. Disponible en: <https://www.kiga-berlin.org> [Fecha de consulta: 30 de noviembre de 2023].

Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Disponible en: <https://eur-lex.europa.eu/ES/legal-content/glossary/high-representative-of-the-union-for-foreign-affairs-and-security-policy.html#:~:text=El%20actual%20AR%20es%20Josep,un%20per%C3%ADodo%20de%20cinco%20años.> [Fecha de consulta: 22 de noviembre de 2023].

Applied Intelligence and Data Analysis (AIDA). Disponible en: <https://aida.etsisi.upm.es> [Fecha de consulta: 30 de noviembre de 2023].

A Strategic Compass for the EU. Disponible en: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en [Fecha de consulta: 03 de noviembre de 2023].

«Brian Fishman», *New America*. Disponible en: <https://www.newamerica.org/our-people/brian-fishman/> [Fecha de consulta: 02 de diciembre de 2023].

«Cambios en el Código Penal tras la aprobación de la ley del "solo sí es sí"», Gerson Vidal Rodríguez, 29 de mayo de 2023. Disponible en: <https://www.gersonvidal.com/blog/cambios-codigo-penal-ley-solo-si-es-si/> [Fecha de consulta: 13 de diciembre de 2023].

«Channel Program», *GOV.UK*. Disponible en: <https://www.gov.uk/government/publications/channel-and-prevent-multi-agency-panel-pmap-guidance> [Fecha de consulta: 29 de diciembre de 2023].

Christchurch Call. Disponible en: <https://www.christchurchcall.com> [Fecha de consulta: 11 de diciembre de 2023].

Comisaría General de Información, *Policía Nacional*. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cginformacion.php [Fecha de consulta: 22 de noviembre de 2023].

Comisaría General de Policía Judicial, *Policía Nacional*. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php [Fecha de consulta: 22 de noviembre de 2023].

Comité Europeo de las Regiones. Disponible en: <https://cor.europa.eu/es> [Fecha de consulta: 22 de noviembre de 2023].

«Common Travel Area: rights of UK and Irish citizens Information for UK and Irish citizens on their rights under the Common Travel Area arrangements (CTA)», *Home Office*. Disponible en: <https://www.gov.uk/government/publications/common-travel-area-guidance> [Fecha de consulta: 29 de diciembre de 2023].

Community Counteracting Radicalisation (CoCoRa). Disponible en: www.mhtconsult.dk y www.cesie.org [Fecha de consulta: 30 de noviembre de 2023].

Community Policing Preventing Radicalisation (CoPPRa). Disponible en: https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/copptra_en [Fecha de consulta: 30 de noviembre de 2023].

«Cómo denunciar contenido ilegal», *TikTok*. Disponible en: <https://www.tiktok.com/legal/page/global/reporting-illegal-content/es> [Fecha de consulta: 04 de diciembre de 2023].

Comunicado web del Departamento de Seguridad Nacional de España, Europol pone en marcha el Centro Europeo Contra el Terrorismo (ECTC), en <https://www.dsn.gob.es/en/actualidad/sala-prensa/europol-pone-marcha-centro-europeo-contraterrorismo-ectc>

«Condiciones de uso de Instagram», *Instagram*. Disponible en: https://help.instagram.com/581066165581870/?locale=es_ES [Fecha de consulta: 04 de diciembre de 2023].

Consejo de Europa. <https://www.coe.int/es/web/about-us/who-we-are> [Fecha de consulta: 22 de noviembre de 2023].

Counter Terrorism Security Adviser (CTSA). Disponible en: <https://www.police.uk/pu/contact-us/possible-terrorist-activity/contact-a-counter-terrorism-security-adviser-ctsa/?tid=911378&lid=&cid=&rid=&stepid=1> [Fecha de consulta: 11 de diciembre de 2023].

Counter Terrorism Policing (CTP). Disponible en: <https://www.counterterrorism.police.uk> [Fecha de consulta: 10 de diciembre de 2023].

«Díaz Ayuso invita a conocer la Comunidad de Madrid ‘al servicio de España’ con ‘el mejor escenario cultural que nadie pueda imaginar’», *Portal de la Comunidad de Madrid*. Disponible en: <https://www.comunidad.madrid/noticias/2024/01/26/diaz-ayuso-invita-conocer-comunidad-madrid-servicio-espana-mejor-escenario-cultural-nadie-pueda-imaginar> [Fecha de consulta: 26 de enero de 2024].

Discurso ante la sesión plenaria del Parlamento Europeo (2019): *Discurso pronunciado por Ursula von der Leyen, Presidenta electa de la Comisión Europea*, 27 de noviembre de 2019, p. 7. Disponible en: https://commission.europa.eu/system/files/2019-11/president-elect-speech_es.pdf [Fecha de consulta: 09 de noviembre de 2023].

«El Gobierno hace pública por primera vez la Estrategia Nacional contra el Terrorismo», *La Moncloa*, 26 de febrero de 2019. Disponible en: <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2019/260219-estrategia.aspx> [Fecha de consulta: 23 de noviembre de 2023].

Educate.against.hate, *Department for Education and the Home Office, UK*. Disponible en: <https://www.educateagainsthate.com/prevent-training/> [Fecha de consulta: 29 de diciembre de 2023].

«España y Europol lideran la retirada de más de 2.000 contenidos terroristas de TikTok», *Ministerio del Interior*, 5 octubre 2023. Disponible en: <https://www.interior.gob.es/opencms/en/detail-pages/article/Espana-y-Europol-lideran-la-retirada-de-mas-de-2.000-contenidos-terroristas-de-TikTok/> [Fecha de consulta: 02 de diciembre de 2023].

Estrategia de Ciberseguridad. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-strategy> [Fecha de consulta: 12 de noviembre de 2023].

«EU law enforcement and judicial authorities join forces to disrupt terrorist propaganda online», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online> [Fecha de consulta: 02 de diciembre de 2023].

«European Centre for Algorithmic Transparency», *Comisión Europea*. Disponible en: https://algorithmic-transparency.ec.europa.eu/index_en [Fecha de consulta: 04 de diciembre de 2023].

«Europol and Telegram take on terrorist propaganda online», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online> [Fecha de consulta: 01 de diciembre de 2023].

«Europol and TikTok collaborate to bolster efforts against terrorist content», *CT Insight*, 5 octubre 2023. Disponible en: <https://ctinsight.net/europol-and-tiktok-collaborate-to-bolster-efforts-against-terrorist-content/> [Fecha de consulta: 02 de diciembre de 2023].

«Europol and TikTok collaborate to bolster efforts against terrorist content», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-tiktok-collaborate-to-bolster-efforts-against-terrorist-content#:~:text=On%2028%20September%2C%20a%20large,and%20violent%20extremist%20content%20online>. [Fecha de consulta: 02 de diciembre de 2023].

EU Terrorism Situation & Trend Report (TE-SAT). Disponible en: <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [Fecha de consulta: 22 de noviembre de 2023].

EXIT-Deutschland. Disponible en: <https://www.buendnis-toleranz.de/archiv/themen/extremismus/161709/exit-deutschland> [Fecha de consulta: 1 de diciembre de 2023].

«Extremist Content Online: TamTam Edition. Messenger Platform Is Home To Content Promoting Neo-Nazi Accelerationism And Acts Of Terrorism», *Counter Extremism Project (CEP)*. Disponible en: <https://www.counterextremism.com/press/extremist-content-online-tamtam-edition> [Fecha de consulta: 01 de diciembre de 2023].

FEDERAL MINISTRY OF DEFENCE (2022): National Security Strategy, Germany. Strategic Concept 2022. Disponible en: <https://www.bmvg.de/en/national-security-policy> [Fecha de consulta: 29 de noviembre de 2023].

Fijación de las prioridades políticas de la UE. Disponible en: <https://www.consilium.europa.eu/es/european-council/role-setting-eu-political-agenda/> [Fecha de consulta: 22 de noviembre de 2023].

Fondo Europeo de Apoyo a la Paz. Disponible en: <https://www.consilium.europa.eu/es/policies/european-peace-facility/> [Fecha de consulta: 03 de noviembre de 2023].

Fondo Europeo de Defensa (EDF). Disponible en: [https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-\(edf\)](https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)) [Fecha de consulta: 03 de noviembre de 2023].

Forschungswerkstatt Salam-Online, Zentrum für Islamische Theologie (ZIT), Universität Münster. Disponible en: <https://www.uni-muenster.de/ZIT/Religionspaedagogik/Projekte/salam-online.html> [Fecha de consulta: 1 de diciembre de 2023].

«Francisco Martínez afirma en Luxemburgo ante la industria de Internet que la "colaboración público-privada es una herramienta clave en la lucha contra el yihadismo" en la Red», *La Moncloa*, 9 de octubre de 2014. Disponible en: <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2014/101014jailuxemburgo.aspx> [Fecha de consulta: 21 de septiembre de 2022].

Gemeinsames Terrorismusabwehrzentrum, GTAZ. (Centro Conjunto Contra el Terrorismo). Disponible en: https://www.bka.de/DE/UnsereAufgaben/Kooperationen/GTAZ/gtaz_node.html [Fecha de consulta: 1 de diciembre de 2023].

«GDT Grupo de Delitos Informáticos», *Guardia Civil*. Disponible en: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php [Fecha de consulta: 22 de noviembre de 2023].

Global Internet Forum to Counter Terrorism (GIFCT). Disponible en: <https://gifct.org> [Fecha de consulta: 11 de diciembre de 2023].

«Grupo táctico de operaciones aéreas especiales para la Fuerza de Respuesta Rápida de la OTAN», *Ministerio de Defensa*. Disponible en: <https://ejercitodelaire.defensa.gob.es/EA/ejercitodelaire/es/noticias/noticia/Grupo-tactico-de->

[operaciones-aereas-especiales-para-la-Fuerza-de-Respuesta-Rapida-de-la-OTAN/](#) [Fecha de consulta: 13 de noviembre de 2023].

«Guidance: Making a referral to Prevent», *GOV.UK*. Disponible en: <https://www.gov.uk/guidance/making-a-referral-to-prevent> [Fecha de consulta: 29 de diciembre de 2023].

Home Office in the media. Updated CONTEST strategy published. Fact Sheet: Multi-Agency Centre (MAC). Disponible en: <https://homeofficemedia.blog.gov.uk/2018/06/04/updated-contest-strategy-published/> [Fecha de consulta: 11 de diciembre de 2023].

«How is Europol keeping online spaces safe?», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/how-europol-keeping-online-spaces-safe> [Fecha de consulta: 29 de noviembre de 2023].

«Independent Reviewer of State Threat Legislation appointed», *Home Office*. Disponible en: <https://www.gov.uk/government/news/independent-reviewer-of-state-threat-legislation-appointed#:~:text=It%20is%20a%20new%20role,report%20their%20findings%20and%20recommendations>. [Fecha de consulta: 29 de diciembre de 2023].

«Informe de actividad 2019 de la Unidad de Referencia de Internet (IRU) de la Unión Europea», *Departamento de Seguridad Nacional (DSN) del Gobierno de España*, Disponible en: <https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-actividad-2019-unidad-referencia-internet-iru-union-europea> [Fecha de consulta: 01 de diciembre de 2023].

International Institute for Human Rights and Peace. Disponible en: www.2idhp.eu [Fecha de consulta: 30 de noviembre de 2023].

INTERPOL. *Alentamos el uso de terminología apropiada para evitar banalizar el abuso y la explotación sexual de niños*. Disponible en: <https://www.interpol.int/es/Delitos/Delitos-contramenores/Terminologia-apropiada> [Fecha de consulta: 23 de noviembre de 2023].

JAMIL, Verein zur Förderung akzeptierender Jugendarbeit, Bremen. Disponible en: <https://vaja-bremen.de/teams/jamil/> [Fecha de consulta: 1 de diciembre de 2023].

JENKINS, Henry (2023): «Transmedia Storytelling», *MIT Technology Review*, *Humans and Technology*. Disponible en: <https://www.technologyreview.com/2003/01/15/234540/transmedia-storytelling/> [Fecha de consulta: 23 de junio de 2023].

Joint Statement by United States Secretary of Homeland Security Mayorkas and European Union Commissioner for Internal Market Breton. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_394 [Fecha de consulta: 22 de noviembre de 2023].

Joint Terrorism Analysis Centre (JTAC). Disponible en: <https://www.mi5.gov.uk/joint-terrorism-analysis-centre> [Fecha de consulta: 10 de diciembre de 2023].

La Secreta de Franco: ya era hora de investigar a la Brigada Político Social», *Conversaciones sobre Historia*, 21 de abril de 2022. Disponible en: <https://conversacionsobrehistoria.info/2022/04/21/la-secreta-de-franco-ya-era-hora-de-investigar-a-la-brigada-politico-social/> [Fecha de consulta: 22 de diciembre de 2022].

«Llamamiento de Christchurch para eliminar el contenido terrorista y extremista violento de la red (15 de mayo de 2019)», *Ministère de l'Europe et des Affaires étrangères, France Diplomatie*. Disponible en: <https://www.diplomatie.gouv.fr/es/politica-exterior/diplomacia-digital/eventos/articulo/llamamiento-de-christchurch-para-eliminar-el-contenido-terrorista-y-extremista> [Fecha de consulta: 11 de diciembre de 2023].

"Live Democracy!" ("Vive la Democracia"). Bundesministerium für Familie, Senioren, Frauen und Jugend, BMFSFJ. Disponible en: <https://www.demokratie-leben.de/en/programme> [Fecha de consulta: 1 de diciembre de 2023].

London Is Open. Disponible en: <https://www.london.gov.uk/london-open> [Fecha de consulta: 29 de diciembre de 2023].

LÓPEZ NALDA, María/BOULAT, Pierre (2015): «El Estado Islámico, ¿puede considerarse un Estado según el Derecho internacional?», *Legal Today*. Disponible en: <https://www.legaltoday.com/practica-juridica/derecho-internacional/derecho-union-europea/el-estado-islamico-puede-considerarse-un-estado-segun-el-derecho-internacional-2015-04-22/> [Fecha de consulta: 23 de junio de 2023].

MARTÍNEZ PERZA, Carmen. «La reforma del Código Penal de 2010», *Derecho Penitenciario*, artículo de opinión, pp. 18-26. Disponible en: <http://www.derechopenitenciario.com/comun/fichero.asp?id=2160> [Fecha de consulta: 3 de diciembre de 2023].

Media Actie Kuregem Stad (MAKS VZW). Disponible en: www.maksvzw.org [Fecha de consulta: 30 de noviembre de 2023].

«New statistics show increase in Prevent referrals», *Counter Terrorism Policing*. Disponible en: <https://www.counterterrorism.police.uk/new-statistics-show-increase-in-prevent-referrals/> [Fecha de consulta: 29 de diciembre de 2023].

«Nuestras unidades de operaciones aéreas especiales: helicópteros, paracaidistas y mucho más», *Aviación militar*, edición online de 19 de junio de 2023. Disponible en: <https://aviacionmilitar.es/nuestras-unidades-de-operaciones-aereas-especiales-helicopteros-paracaidistas-y-mucho-mas> [Fecha de consulta: 13 de noviembre de 2023].

«Operación de Europol dirigida al contenido terrorista en línea», *OIPOL*. Disponible en: <https://oipol.org/2022/02/03/operacion-de-europol-dirigida-al-contenido-terrorista-en-linea/> [Fecha de consulta: 29 de noviembre de 2023].

Pädagogik zwischen Islam, Islamfeindlichkeit und Islamismus. (Pedagogía, Educación Cívica y Prevención). Disponible en: <http://www.ufuq.de> [Fecha de consulta: 1 de diciembre de 2023].

«Paquete de la Ley de Servicios Digitales», Comisión Europea, 25 de septiembre de 2023. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package> [Fecha de consulta: 03 de diciembre de 2023].

«Proscribed terrorist groups or organisations», *Home Office*. Disponible en: <https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version#list-of-proscribed-international-terrorist-groups> [Fecha de consulta: 19 de enero de 2024].

QUILLIAM FOUNDATION. Disponible en: <http://www.quilliamfoundation.org> [Disponible hasta año 2020. Última fecha de consulta: año 2019].

RADEQUAL. Disponible en: <https://www.manchester.gov.uk/makingmcrafer/info/6/work/6/radequal-rethinking-radicalisation-programme> [Fecha de consulta: 29 de diciembre de 2023].

«Radicalisation Awareness Network», *Real Instituto Elcano*. Disponible en: <https://www.realinstitutoelcano.org/en/projects/radicalisation-awareness-network/> [Fecha de consulta: 30 de noviembre de 2023].

«RAN Policy Support», *European Commission*. Disponible en: https://home-affairs.ec.europa.eu/networks/ran-policy-support_en [Fecha de consulta: 30 de noviembre de 2023].

«Referral Action Day against Islamic State online terrorist propaganda», *Europol*. Disponible en: <https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda> [Fecha de consulta: 01 de diciembre de 2023].

Revisión Anual Coordinada de la Defensa (*CARD, Coordinated Annual Review on Defence*). Disponible en: [https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-\(card\)](https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)) [Fecha de consulta: 03 de noviembre de 2023].

Sawab. Disponible en: <https://sawabcenter.org> [Fecha de consulta: 24 de noviembre de 2023].

SIRIUS. Disponible en: <https://www.europol.europa.eu/operations-services-innovation/sirius-project#:~:text=SIRIUS%20is%20an%20EU%2Dfunded,of%20criminal%20investigations%20and%20proceedings> [Fecha de consulta: 03 de noviembre de 2023].

Stad Vilvoorde. Disponible en: www.vilvoorde.be [Fecha de consulta: 30 de noviembre de 2023].

Stop Radicalismos, *Ministerio del Interior. Gobierno de España*. Disponible en: <https://stop-radicalismos.ses.mir.es/stop/FormServlet> [Fecha de consulta: 24 de noviembre de 2023].

Strong Cities Networks. Disponible en: <https://strongcitiesnetwork.org> [Fecha de consulta: 24 de noviembre de 2023].

Tech Against Terrorism. Disponible en: <https://techagainstterrorism.org/home> [Fecha de consulta: 11 de diciembre de 2023].

«Telegram Deplatforming ISIS Has Given Them Something to Fight For», *VICE News*. Disponible en: <https://www.vice.com/en/article/vb55bd/telegram-deplatforming-isis-has-given-them-something-to-fight-for> [Fecha de consulta: 02 de diciembre de 2023].

Terrorism and national emergencies. Disponible en: <https://www.gov.uk/terrorism-national-emergency> [Fecha de consulta: 10 de diciembre de 2023].

«The Aarhus Model», *Hedayah*. Disponible en: <https://hedayah.com/program/the-aarhus-model/> [Fecha de consulta: 30 de noviembre de 2023].

The European Cyber Conflict Research Incubator. Disponible en: <https://eccri.eu> [Fecha de consulta: 04 de diciembre de 2023].

«The Russian Social Network Letting ISIS Back Online», *VICE News*. Disponible en: <https://www.vice.com/en/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app> [Fecha de consulta: 02 de diciembre de 2023].

Tipos de legislación de la Unión Europea. Disponible en: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_es [Fecha de consulta: 16 de noviembre de 2023].

Tratado del Atlántico Norte. Disponible en: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=es [Fecha de consulta: 06 de noviembre de 2023].

TUNG, Liam (2008): *Jihadists get World-class encryption kit*. Disponible en: www.zdnet.com.au/jihadist-get-world-class-encryption-kit-339285480.htm [Fecha de consulta: 21 de septiembre de 2020].

«Una Europa Adaptada a la Era Digital. Capacitar a las personas con la ayuda de una nueva generación de tecnologías», *Comisión Europea*. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es [Fecha de consulta: 04 de diciembre de 2023].

Unidad Central de Inteligencia UCI, *Intelpage*. Disponible en: <https://intelpage.info/unidad-central-de-inteligencia-uci.html> [Fecha de consulta: 22 de noviembre de 2023].

Unidad Cibernética Conjunta, *Comisión Europea*. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/joint-cyber-unit> [Fecha de consulta: 12 de noviembre de 2023].

Unidad de Referencia de Internet de la Unión Europea, *Europol*. Disponible en: <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referral-unit-eu-iru> [Fecha de consulta: 29 de noviembre de 2023].

US DEPARTMENT OF STATE. Country Reports on Terrorism 2020: Germany. Disponible en: <https://www.state.gov/reports/country-reports-on-terrorism-2020/germany/> [Fecha de consulta: 29 de noviembre de 2023].

WEIMANN, Gabriel (2008): «Online terrorist prey on the vulnerable», *YaleGlobal Online*. Disponible en: <https://archive-yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable> [Fecha de consulta: 23 noviembre 2023].

«Youth Partnership», *Council of Europe and European Union*. Disponible en: <https://pjp-eu.coe.int/en/web/youth-partnership> [Fecha de consulta: 30 de noviembre de 2023].

FUENTES INFORMATIVAS NO PERIODICAS

DEEN, Adam/ HASAN, Usama (2016, 1 de diciembre). «Teología, Educación y Difusión». [Ponencia]. *Workshop: Políticas y comunicación estratégica para la prevención de la radicalización violenta*. Programa dirigido a profesionales, investigadores y Fuerzas y Cuerpos de Seguridad. Organizado por Ayuntamiento de Málaga, Área de Derechos Sociales, y Escuela de Seguridad Pública del Ayuntamiento de Málaga (ESPAM) y Quilliam, 1 y 2 de diciembre de 2016, Málaga, España.

DEEN, Adam/ MALIK, Nikita (2016, 1 de diciembre). «Políticas y estrategias de comunicación». [Ponencia]. *Workshop: Políticas y comunicación estratégica para la prevención de la radicalización violenta*. Programa dirigido a profesionales, investigadores y Fuerzas y Cuerpos de Seguridad. Organizado por Ayuntamiento de Málaga, Área de Derechos Sociales, y Escuela de Seguridad Pública del Ayuntamiento de Málaga (ESPAM) y Quilliam, 1 y 2 de diciembre de 2016, Málaga, España.

TORREGROSA, Javier (2016, 5 de octubre). «RISK-TRACK: Evaluando el riesgo de radicalización en redes sociales», en: *Jornadas Exclusivas sobre Yihadismo Actual: Uso de la inteligencia en HUMINT Y OSINT*. Organizado por GALEÓN-CISEG, 5 y 6 de octubre de 2016, Sevilla, España.

TORRES SORIANO, Manuel (2023, 16 de noviembre): «Panel 2: Tendencias de la amenaza en las sociedades occidentales», en: *X Foro Elcano Terrorismo Global “La nueva fase del*

terrorismo global: tendencias de la amenaza”, Organizado por el Real Instituto Elcano, 16 de noviembre de 2023, Madrid, España.

FUENTES INFORMATIVAS PERIODICAS

«Alemania prohíbe toda actividad del grupo terrorista libanés Hezbollah», *El periódico de Aragón*, edición online de 30 de abril de 2020. Disponible en: <https://www.elperiodicodearagon.com/internacional/2020/04/30/alemania-prohibe-actividad-grupo-terrorista-46536814.html> [Fecha de consulta: 29 de noviembre de 2023].

«Al Qaeda y Estado Islámico se hacen fuertes en Malí tras la salida de Francia y en plena retirada de la ONU», *Europa Press*. Disponible en: <https://www.europapress.es/internacional/noticia-qaeda-estado-islamico-hacen-fuertes-mali-salida-francia-plena-retirada-onu-20231001083252.html> [Fecha de consulta: 17 de diciembre de 2023].

«Apoyo a los TEDAX de la Policía Nacional», *Revista IIMagina*, edición online de diciembre 2023, Año XIII, N.º 23. Disponible en: https://asociacion11m.org/wp-content/uploads/2023/11/IIMAGINA-23_WEB.pdf [Fecha de consulta: 22 de diciembre de 2022].

«Así es la lista negra de Facebook para individuos y organizaciones peligrosas», *Escudo Digital*, edición online de 3 de octubre de 2021. Disponible en: https://www.escudodigital.com/sociedad/seguridad-y-consumo/asi-es-la-lista-negra-de-facebook-para-individuos-y-organizaciones-peligrosas_34556_102.html [Fecha de consulta: 03 de diciembre de 2023].

BARRANCOS, David (2016): «Así recluta el EI: Ven a jugar al 'Call of Duty' de verdad/Entrevistado por Mayo Cerqueiro, Pablo», *Periódico El Español*, edición online de 15 de septiembre de 2016. Disponible en: https://www.elespanol.com/videojuegos/20151120/80741986_0.html [Fecha de consulta: 23 de junio de 2023].

BORRELL, Josep (2020). «Europa debe aprender rápidamente a hablar el lenguaje del poder. / Entrevistado por J. H. H. Weiler», *Periódico El País*. Disponible en: <https://agendapublica.elpais.com/noticia/16744/borrell-europa-debe-aprender-rapidamente-hablar-lenguaje-poder> [Fecha de consulta: 09 de noviembre de 2023].

«Borrell pide una fuerza militar de la UE: "Estados Unidos ya no hará las guerras de los demás», *El Confidencial*, Disponible en: https://www.elconfidencial.com/mundo/europa/2021-08-22/borrell-critica-que-eeuu-hace_3244478/ edición online de 23 de agosto de 2021. [Fecha de consulta: 09 de noviembre de 2023].

BOUREKBA, Moussa (2020): «La extrema derecha violenta y el yihadismo comparten una misma cosmovisión/ Entrevistado por P. Simón», *Revista La Marea*, edición online de 3 de julio

de 2020. Disponible en <https://www.lamarea.com/2020/07/03/extrema-derecha-violenta-y-yihadismo-comparten-cosmovision/> [Fecha de consulta: 21 de noviembre de 2023].

«Bruselas advierte a TikTok: se expone a multas o un veto temporal si no protege a los menores», *La Vanguardia*, 20 de enero de 2023. Disponible en: <https://www.lavanguardia.com/tecnologia/redes-sociales/20230120/8697009/bruselas-advierte-tiktok-enfrenta-sanciones-e-prohibicion-protege-menores-pmv.html> [Fecha de consulta: 04 de diciembre de 2023].

«El autor del atentado de Londres participaba en una charla sobre reinserción de presos», *Heraldo*, edición online de 30 de noviembre de 2019. Disponible en: <https://www.heraldo.es/noticias/internacional/2019/11/30/la-policia-registra-la-vivienda-del-autor-del-atentado-de-londres-1346676.html> [Fecha de consulta: 29 de diciembre de 2023].

«El autor del atentado en Londres estaba bajo vigilancia tras salir de prisión», *El País*, edición online de 03 de febrero de 2020. Disponible en: https://elpais.com/internacional/2020/02/02/actualidad/1580657288_204017.html [Fecha de consulta: 29 de diciembre de 2023].

«El bastión de defensa de Google en Andalucía», *Diario de Sevilla*, edición online de 4 de diciembre de 2023. Disponible en: https://www.diariodesevilla.es/tecnologia/bastion-defensa-Google-Andalucia-centro-seguridad-malaga-video_0_1853815506.html [Fecha de consulta: 04 de diciembre de 2023].

«El Ejército del Aire reúne en Canarias a 2.000 militares y 35 aeronaves en su principal ejercicio del año», *Revista Mundo militar Infodefensa*, edición online de 19 de octubre de 2022. Disponible en: <https://www.infodefensa.com/texto-diario/mostrar/3930922/ejercito-aire-espacio-da-comienzo-ejercicio-otan-sirio-22> [Fecha de consulta: 13 de noviembre de 2023].

«El ISIS busca nueva plataforma: la Europol asedia su propaganda en Telegram», *El Confidencial*, edición online de 3 de diciembre de 2019. Disponible en: https://www.elconfidencial.com/mundo/2019-12-03/ahogado-por-telegram-el-isis-busca-otras-aplicaciones-para-seguir-con-su-propaganda_2362587/ [Fecha de consulta: 02 de diciembre de 2023].

«El jefe de las SS visita España», *El País*, edición online de 15 de octubre de 2015. Disponible en: https://elpais.com/elpais/2015/10/13/fotorrelato/1444747453_605541.html [Fecha de consulta: 22 de diciembre de 2022].

«España defiende en la UE medidas conjuntas con empresas como Facebook o Twitter para combatir el yihadismo en la red», *Europa Press*, edición online de 3 de julio de 2015. Disponible en: <https://www.europapress.es/nacional/noticia-espana-defiende-ue-medidas-conjuntas-empresas-facebook-twitter-combatir-yihadismo-red-20141009165315.html> [Fecha de consulta: 3 de diciembre de 2023].

«ETA ha modificado su estructura interna por motivos de seguridad», *El Correo*, 23 de marzo de 2006. Disponible en: https://www.elcorreo.com/vizcaya/pg060323/actualidad/politica/200603/23/ECD_eta_funcionamiento.html#&ref=https://www.elcorreo.com/vizcaya/pg060323/actualidad/politica/200603/23/ECD_eta_funcionamiento.html [Fecha de consulta: 22 de diciembre de 2022].

«Europa cambia las reglas de juego para Google, Facebook y TikTok: una inédita ley ya está en vigor y así funciona», *Diario Clarín*, edición online de 25 de agosto de 2023. Disponible en: https://www.clarin.com/mundo/europa-cambia-reglas-juego-google-facebook-tiktok-inedita-ley-vigor-funciona_0_GcDzCUMMnN.html [Fecha de consulta: 04 de diciembre de 2023].

EUROPOL EU IRU OFFICIAL (2020): «A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit/Entrevistado por A. Amarasingam», *CTC Sentinel, Combating Terrorism Center at West Point*, edición online de febrero 2020. Disponible en: <https://ctc.westpoint.edu/view-ct-foxhole-interview-official-europols-eu-internet-referral-unit/> [Fecha de consulta: 01 de noviembre de 2023].

«Europol explica cómo combate la difusión de contenidos terroristas en internet», *Escudo Digital*, edición online de 4 de febrero de 2022. Disponible en: https://www.escudodigital.com/ciberseguridad/europol-bases-combatir-contenidos-terroristas-internet_50273_102.html [Fecha de consulta: 29 de noviembre de 2023].

«Facebook e Instagram permitirán que veas las historias y los reels de forma cronológica», *ABC*, edición online de 22 de agosto de 2023. Disponible en: <https://www.abc.es/tecnologia/redes/facebook-instagram-permitiran-veas-historias-reels-forma-20230822171515-nt.html> [Fecha de consulta: 04 de diciembre de 2023].

«Facebook, Twitter o YouTube deberán retirar contenidos terroristas en una hora en la Unión Europea», *Escudo Digital*, edición online de 10 de Diciembre de 2020. Disponible en: https://www.escudodigital.com/defensa/facebook-twitter-o-youtube-deberan-retirar-contenidos-terroristas-en-una-hora-en-la-union-europea_22127_102.html [Fecha de consulta: 03 de diciembre de 2023].

«Facebook usará inteligencia artificial para combatir las publicaciones extremistas», *New York Times*, edición online de 19 de junio de 2017. Disponible en: <https://www.nytimes.com/es/2017/06/19/espanol/facebook-extremismo-inteligencia-artificial.html> [Fecha de consulta: 03 de diciembre de 2023].

«Google abre en Málaga su primer centro especializado en ciberseguridad de Europa», *El País*, edición online de 29 de noviembre de 2023. Disponible en: <https://elpais.com/tecnologia/2023-11-29/google-abre-en-malaga-su-primer-centro-especializado-en-ciberseguridad-de-europa.html> [Fecha de consulta: 04 de diciembre de 2023].

«Google presenta en Málaga su tercer centro de ciberseguridad de Europa», *Escudo Digital*, edición online de 30 de noviembre de 2023. Disponible en:

https://www.escudodigital.com/ciberseguridad/google-presenta-en-malaga-su-tercer-centro-ciberseguridad-europa_57346_102.html [Fecha de consulta: 04 de diciembre de 2023].

«La entrada irregular de migrantes a la UE por el Mediterráneo central alcanza máximos históricos», *El País*, edición online de 12 de mayo de 2023. Disponible en: <https://elpais.com/internacional/2023-05-12/la-entrada-irregular-de-migrantes-a-la-ue-por-el-mediterraneo-central-alcanza-maximos-historicos.html> [Fecha de consulta: 22 de noviembre de 2023].

«La nueva agencia contra el crimen del Reino Unido acrecienta la búsqueda de delincuentes británicos en España», *Gob.uk*, edición online de 7 de octubre de 2013. Disponible en: <https://www.gov.uk/government/news/197196.es> [Fecha de consulta: 11 de diciembre de 2023].

«La UE aprueba una nueva ley para frenar el contenido ilegal de plataformas como Facebook, Google o Amazon», *La Voz de Galicia*, edición online de 23 de abril de 2022. Disponible en: <https://www.lavozdegalicia.es/noticia/sociedad/2022/04/23/ue-aprueba-nueva-ley-frenar-contenido-ilegal-plataformas-facebook-google-amazon/00031650700928811380708.htm> [Fecha de consulta: 04 de diciembre de 2023].

«La Unión Europea impondrá controles más estrictos a las grandes plataformas digitales», *Euronews*, edición online de 25 de abril de 2023. Disponible en: <https://es.euronews.com/my-europe/2023/04/25/la-ue-impondra-controles-mas-estrictos-a-las-grandes-plataformas-digitales> [Fecha de consulta: 03 de diciembre de 2023].

«La Unión Europea reforzará el control de fronteras e Internet», *Diario de Navarra*, edición online de 11 de enero de 2015. Disponible en: <https://www.noticiasdenavarra.com/mundo/2015/01/11/ue-reforzara-control-fronteras-exteriores-2930972.html> [Fecha de consulta: 03 de noviembre 2023].

«Londres llora a las últimas víctimas del terrorismo yihadista», *La Razón*, edición online de 2 de diciembre de 2019. Disponible en: <https://www.larazon.es/internacional/20191202/amlirlo2gfauzexjedrcnngijy.html> [Fecha de consulta: 29 de diciembre de 2023].

«Los 'ciberpolicías' de España: así es la Brigada Central de Investigación Tecnológica», *Periódico 20 minutos*, edición online de 20 de enero de 2023. Disponible en: <https://www.20minutos.es/tecnologia/ciberseguridad/quien-es-y-como-actua-la-policia-cibernetica-en-espana-5093449/> [Fecha de consulta: 23 de noviembre de 2023].

«Messaging app TamTam used for IS propaganda dissemination», *BBC Monitoring*, edición online de 07 de Abril de 2018. Disponible en: <https://monitoring.bbc.co.uk/product/c1dp1qli> [Fecha de consulta: 02 de diciembre de 2023].

«Por qué la Unión Europea no tiene un ejército propio y qué son los 'battlegroups' de la UE», *AS España*, edición online de 28 de febrero de 2022. Disponible en:

https://as.com/diarioas/2022/02/28/actualidad/1646032381_346464.html [Fecha de consulta: 09 de noviembre de 2023].

«Posible "desmilitarización" de la Policía Armada», *El País*, edición online de 8 de junio de 1977. Disponible en: https://elpais.com/diario/1977/06/08/espana/234568804_850215.html [Fecha de consulta: 22 de diciembre de 2022].

«Radicalism: Internet. Question for Home Office», *UK Parliament*, edición online de 28 de junio de 2017. Disponible en: <https://questions-statements.parliament.uk/written-questions/detail/2017-06-28/1708> [Fecha de consulta: 11 de diciembre de 2023].

«Reino Unido eleva a ‘crítico’ su nivel de alerta terrorista y espera un ataque ‘inminente’ tras el atentado de Manchester», *BBC News*, edición online de 23 de mayo de 2017. Disponible en: <https://www.bbc.com/mundo/noticias-internacional-40023305> [Fecha de consulta: 10 de diciembre de 2023].

«Reino Unido presenta ley de emergencia al Parlamento», *Anadolu Ajansi*, edición online de 12 de febrero de 2020. Disponible en: <https://www.aa.com.tr/es/pol%C3%ADtica/reino-unido-presenta-ley-de-emergencia-al-parlamento/1731326> [Fecha de consulta: 29 de diciembre de 2023].

«The Centre for the Protection of National Infrastructure (CPNI) has evolved to become the National Protective Security Authority (NPSA)», *Protect UK*, edición online de 17 de marzo de 2023. Disponible en: <https://lc.cx/wpsK3U> [Fecha de consulta: 11 de diciembre de 2023].

«The day the world changed», *The Economist*, edición online de 13 de Septiembre de 2001. Disponible en: <https://www.economist.com/leaders/2001/09/13/the-day-the-world-changed> [Fecha de consulta: 13 de noviembre de 2013].

TORRENS, Xavier (2023): «El islamismo radical se caracteriza por su racismo anti-occidental/ Entrevistado por I. Ellakuría», *Periódico El Mundo*, edición online de 29 de enero de 2023. Disponible en: <https://www.elmundo.es/espana/2023/01/29/63d53b27e4d4d89f7c8b456e.html> [Fecha de consulta: 21 de noviembre de 2023].

«UE debe aceptar intervenir Skype para evitar vuelta de insurgentes», *Noticia de Reuters*, edición online de 06 de febrero de 2015. Disponible en: <https://www.reuters.com/article/oesen-ue-skype-seguridad-idESKBN0LA1QM20150206/> [Fecha de consulta: 29 de noviembre de 2023].

«Un comando de geos patrulla de incógnito las calles de Madrid para abatir yihadistas», *El Confidencial*, edición online de 29 de agosto de 2017. Disponible en: https://www.elconfidencial.com/espana/2017-08-28/geo-abatir-patrulla-operacion-madrid_1434118/ [Fecha de consulta: 21 de septiembre de 2022].

FUENTES NORMATIVAS

[20] (2), Propuesta de Decisión Marco del Consejo sobre la lucha contra el terrorismo, COM/2001/0521 final, CNS 2001/0217 Diario Oficial N.º 332 E de 27/11/2001, p. 0300-0304. 52001PC0521.

Anti-Terrorism, Crime and Security Act 2001 [ATCS Act 2001]. (Ley contra el Terrorismo, la Delincuencia y la Seguridad [ATCS] de 2001, Reino Unido).

Bundeskriminalamtgesetz (Ley de la Oficina Federal de Policía Criminal).

Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 1 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 413) geändert worden ist. (Ley Federal de Protección Constitucional de 20 de diciembre de 1990 (BGBl. I p. 2954, 2970), modificada por última vez por el artículo 1 de la Ley de 22 de diciembre de 2023 (BGBl. 2023 I No. 413)).

Bundeszentralregistergesetz (BZRG). Ley del Registro Central Federal (BZRG).

Código Penal Español.

CONSEJO DE EUROPA (1977): Convenio Europeo de Estrasburgo para la represión del terrorismo, Serie de Tratados N.º 090, de 27 de enero de 1977.

CONSEJO DE EUROPA (2001): Convenio sobre la Ciberdelincuencia, Serie de Tratados N.º 185, de 23 de noviembre de 2001.

CONSEJO DE EUROPA (2003): Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, Serie de Tratados N.º 189, de 28 de enero de 2003.

CONSEJO DE EUROPA (2005): Convenio del Consejo de Europa para la prevención del terrorismo, Varsovia, 16 de mayo de 2005.

CONSEJO DE EUROPA (2015): Protocolo adicional al Convenio del Consejo de Europa para la prevención del terrorismo, Riga, 22 de octubre de 2015, (DOUE de 22 de junio de 2018).

Convención Interamericana contra el Terrorismo, AG/RES. 1840 (XXXII-O/02), aprobada en la primera sesión plenaria, celebrada el 3 de junio de 2002.

Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

Counter-Terrorism and Border Security Act 2019 (Ley de Seguridad Fronteriza y Antiterrorismo de 2019, Reino Unido).

Counter-Terrorism and Sentencing Act 2021 (Ley de Sentencias y Antiterrorismo de 2021, Reino Unido).

Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906).

Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

Decisión 2005/681/JAI del Consejo, de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI.

Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (EUROPOL).

Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008 por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (DO L 164 de 22.6.2002).

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

Decisión (UE) 2018/890 relativa a la celebración, en nombre de la Unión Europea, del Protocolo Adicional al Convenio del Consejo de Europa para la prevención del terrorismo.

Decreto ley 10/1975, de 26 de agosto, sobre prevención del terrorismo, España.

Directiva 2011/93/UE

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.

Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la DM 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo.

Entwurf eines Gesetzes zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (GVVG-Änderungsgesetz - GVVG-ÄndG), vom 05.02.2015. (Ley de Enmienda sobre el Enjuiciamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado).

Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) (Ley del Servicio Federal de Inteligencia). Última modificación: BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 1 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 410) geändert worden ist, (Ley del BND de 20 de diciembre de 1990 (BGBl. I p. 2954, 2979), modificada por última vez por el artículo 1 de la ley de 22 de diciembre de 2023 (BGBl. 2023 I No. 410)).

Gesetz über den militärischen Abschirmdienst (MAD-Gesetz - MADG). (Ley del Servicio de Contrainteligencia Militar).

Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG) § 2 Grenzschutz (Ley de la Policía Federal, BPolG. Artículo 2 Protección de fronteras).

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen, Sicherheitsüberprüfungsgesetz - SÜG) (Ley sobre los requisitos y el procedimiento para los controles federales de seguridad y la protección de información clasificada, Ley de Control de Seguridad - SÜG).

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG). Ley sobre cédulas de identidad y prueba electrónica de identidad (Ley de cédulas de identidad - PAuswG).

Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus, G.v. (Boletín Oficial Federal I, 26 de julio de 2016, página 1818 (Nº 37); Válido a partir del 30 de julio de 2016).

Gesetz zur Bekämpfung des internationalen Terrorismus, Terrorismusbekämpfungsgesetz (Ley de Lucha contra el Terrorismo Internacional).

Gesetz zur Regelung des öffentlichen Vereinsrechts (Vereinsgesetz). Ley que regula el derecho de asociaciones públicas (Ley de Asociaciones).

Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (GVVG) vom 30.07.2009. (Ley sobre el Procesamiento de la Preparación de Delitos Violentos Graves que ponen en peligro al Estado).

Grundgesetz (Ley Fundamental de la República Federal de Alemania).

Ley 56/1978, de 4 de diciembre, de medidas especiales en relación con los delitos de terrorismo cometidos por grupos armados.

Ley 82/1978, de 28 de diciembre, de modificación del Código Penal en materia de terrorismo.

Ley Orgánica 2/1981, de 4 de mayo, que modifica y adiciona determinados artículos del Código Penal y el de Justicia Militar.

Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

Ley Orgánica 3/1988, de 25 de mayo, de Reforma del Código Penal.

Ley Orgánica 9/1984, de 26 de diciembre, contra la actuación de bandas armadas y elementos terroristas y de desarrollo del artículo 55.2 de la Constitución.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

Ley Orgánica 11/1980, de 1 de diciembre, sobre los supuestos previstos en el artículo 55, 2, de la Constitución.

Luftverkehrsgesetz (LuftVG). Ley de aviación (LuftVG).

Nationality and Borders Act 2022 (Ley de Nacionalidad y Fronteras de 2022, Reino Unido).

National Security Act 2023 (Ley de Seguridad Nacional de 2023, Reino Unido).

Orden PCI/179/2019, de 22 de febrero, por la que se publica la Estrategia Nacional contra el Terrorismo 2019, aprobado por el Consejo de Seguridad Nacional.

Paßgesetz, PaßG (Ley de pasaportes, PassG).

Policing and Crime Act 2017 (Ley de Policía y Crimen de 2017, Reino Unido).

Posición (UE) n.º 8/2016 del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (2016/C 169/02).

Preámbulo de Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Publicada en el BOE núm. 77, de 31 de marzo.

R c. Tsouli y otros. [2007] EWCA (Crim) 3300.

Real Decreto-ley 1/1977, de 4 de enero, por el que se crea la Audiencia Nacional.

Real Decreto-ley 3/1979, de 26 de enero, sobre protección de la seguridad ciudadana.

Real Decreto-ley 21/1978, de 30 de junio, sobre medidas en relación con los delitos cometidos por grupos o bandas armados.

Reglamento de Ejecución (UE) N.º 261/2013 del Consejo de 21 de marzo de 2013.

Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial, art. 7.6.a

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad). ENISA colabora no solo con todos los actores de la UE, sino también con organismos internacionales, como la OCDE, OSCE y OTAN a fin de detectar ciberamenazas, (art. 42).

REGLAMENTO (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea.

REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales).

Resolución del Consejo de Seguridad. S/RES/2170 (2015), 15 de agosto de 2014.

Resolución del Consejo de Seguridad. S/RES/2178 (2014), 24 de septiembre de 2014.

Security and Counter-Terrorism Act of 2015 (Ley de Seguridad y contra el Terrorismo de 2015, Reino Unido).

Sentencia C-646 de 2001 emitida por la Corte Constitucional de Colombia.

Sentencia de 4 de mayo de 2012, causa núm. 0926639036 del Tribunal de Grande Instance de Paris (14ª Cámara/2), Paris.

Sentencia de la Audiencia Nacional, Sala de lo Penal, Res. 25/2016 (AN Penal 28 sep. 2016), España.

Sentencia del Tribunal Constitucional 199/1987, 16 de Diciembre de 1987, España.

Sentencia del Tribunal de Justicia de 5 de febrero de 1963. NV Algemene Transport- en Expeditie Onderneming van Gend & Loos contra Administración fiscal holandesa.

Sentencia del Tribunal de Justicia de 15 de julio de 1964. Flaminio Costa contra E.N.E.L.
Petición de decisión prejudicial: Giudice conciliatore di Milano - Italia. Asunto 6-64.

Strafgesetzbuch (Código Penal Alemán).

Terrorism Act 2000 (Ley contra el Terrorismo de 2000, Reino Unido).

Terrorism Act 2006 (Ley contra el Terrorismo de 2006, Reino Unido).

Terrorist Offenders [Restriction of Early Release] Act 2020 (Ley de Delincuentes Terroristas [Restricción de la Liberación Anticipada] de 2020, Reino Unido).

Terrorism [United Nations Measures] Order 2006 (SI 2006/2657) (Orden contra el Terrorismo de 2006 (SI 2006/2657)).

Tratado de la Unión Europea (TUE)

Tratado de Funcionamiento de la Unión Europea (TFU)

UN. Doc. A/58/612, de 28 de noviembre de 2003.

UN. Doc. A/59/565, de 2 de diciembre de 2004.

UN. A/RES/60/288

UN. A/60/825

UN. A/RES/67/27, de 3 diciembre 2012.

UN. S/RES/2178, 24 September 2014

Vigésimo Tercera Consulta de Ministros de Relaciones Exteriores “Fortalecimiento de la cooperación hemisférica para prevenir, combatir y eliminar el terrorismo”, Organización de los Estados Americanos, RC.23/RES.1/01 rev. 1 corr. 1, aprobada en la primera sesión plenaria, celebrada el 21 de septiembre de 2001.

Vigésimo Cuarta Consulta de Ministros de Relaciones Exteriores “Amenaza Terrorista en las Américas”, Organización de los Estados Americanos, OEA/Ser.F/II.24, RC.24/RES.1/01, aprobada en la primera sesión plenaria, celebrada el 21 de septiembre de 2001.

Zehntes Buch Sozialgesetzbuch, Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X). Libro Décimo del Código Social, Procedimientos Administrativos Sociales y Protección de Datos Sociales (SGB X).

GLOSARIO INSTITUCIONAL DE LA POLÍTICA CRIMINAL DE LA UE

AGENCIAS EUROPEAS

Las Agencias Europeas son organismos internos que han sido creados por medio de un acto de Derecho derivado de la Unión Europea para desempeñar una función específica. Si bien las agencias pueden ser categorizadas por las materias de las que se ocupan, en términos generales las agencias son de dos tipos.

Por un lado, existen las agencias ejecutivas sobre las que recae la gestión de uno o varios programas de la Unión. Las agencias ejecutivas son creadas *ad hoc*, por un tiempo establecido, y trabajan en iniciativas propias de la Comisión Europea. La sede de estas agencias suele estar precisamente dentro de la Comisión, en las oficinas de Bruselas o Luxemburgo.

Por otro lado, nos encontramos con las agencias descentralizadas. Estas agencias, son las que se referencian habitualmente como agencias o agencias europeas, y son organismos que poseen personalidad jurídica propia y operan con independencia.

Estas agencias poseen una misión específica dentro de la Unión Europea, son de naturaleza técnica o científica, y son determinantes para el cumplimiento de los objetivos de la Unión Europea. Las agencias descentralizadas no son Instituciones de la UE, como sí lo son el Consejo, el Parlamento, la Comisión, etc., sino que son organismos descentralizados creados para el cumplimiento de tareas y objetivos concretos en una materia específica dentro de la Unión.

Actualmente existen más de treinta agencias europeas y se encuentran distribuidas por toda Europa. Aquellas que son determinantes en materia de seguridad y que ayuda a crear la Política Criminal de la Unión Europea con relación al terrorismo yihadista en Internet son, entre otras, la Agencia de la Unión Europea para la Cooperación Policial (Europol), la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust), la Agencia de la Unión Europea para la Formación Policial (Cepol), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), y la Agencia Europea de Defensa (EDA).

AR (ALTO REPRESENTANTE DE LA UE PARA ASUNTOS EXTERIORES Y POLÍTICA DE SEGURIDAD)

En Eur-Lex se describe que el cargo de AR fue creado en 1997 en el marco del Tratado de Ámsterdam y su primer titular fue Javier Solana⁸⁶¹, Secretario General del Consejo de la Unión Europea. Años después, el Tratado de Lisboa, que entró en vigor en diciembre de 2009, mantuvo las funciones del AR, pero con un mandato más amplio que incluye la presidencia del Consejo de Asuntos Exteriores y el cargo de vicepresidente de la Comisión.

Sobre el Alto Representante (AR) recae la función de elaborar y dirigir la Política Exterior y de Seguridad Común (PESC) de la UE y la Política Común de Seguridad y Defensa (PCSD);

⁸⁶¹ Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Disponible en: <https://eur-lex.europa.eu/ES/legal-content/glossary/high-representative-of-the-union-for-foreign-affairs-and-security-policy.html#:~:text=El%20actual%20AR%20es%20Josep.un%20per%C3%ADodo%20de%20cinco%20años>. [Fecha de consulta: 22 de noviembre de 2023].

también se encarga de presidir el Consejo de Asuntos Exteriores y de dirigir la Agencia Europea de Defensa (EDA). Es, además, uno de los vicepresidentes de la Comisión Europea, de ahí que se utilice la doble nomenclatura AR/VP para referirse a ambos cargos.

En términos generales, el AR se encarga de coordinar y garantizar que la Acción Exterior de la Unión Europea sea coherente y se oriente siempre hacia un objetivo de seguridad común. El AR desempeña un papel fundamental en la definición y el seguimiento de la respuesta de la UE frente a una crisis en el escenario europeo o internacional que involucre implementar y sostener acciones de seguridad y defensa.

Por otra parte, sus funciones dentro de la Comisión Europea atienden al cumplimiento de objetivos de las relaciones exteriores de la Unión. Esta última es una función con un prisma internacionalista orientada al diálogo político con diversos actores del Sistema internacional. En el marco de esta función se desarrolla la acción y coordinación de todos los intereses diplomáticos de la UE. Para desempeñar esta función, el AR recibe asistencia del Servicio Europeo de Acción Exterior (SEAE).

El actual AR es Josep Borrell Fontelles, que fue nombrado en diciembre de 2019 para un período de cinco años. Sucedió en el cargo a Federica Mogherini (2014-2019), Catherine Ashton (2009-14) y Javier Solana (1999-2009).

CEPOL (AGENCIA DE LA UNIÓN EUROPEA PARA LA FORMACIÓN POLICIAL)

CEPOL es una agencia de la Unión Europea que promueve la cooperación policial europea e internacional por medio de la formación.

Ha sido conocida inicialmente como Escuela Europea de Policía⁸⁶², pero tras el 1 de julio de 2016, fecha de inicio de su nuevo mandato jurídico⁸⁶³, paso a denominarse Agencia de la Unión Europea para la Formación Policial (CEPOL).

CEPOL se dedica a desarrollar, implementar y coordinar formaciones dirigidas a agentes con funciones policiales. Esta agencia contribuye en el desarrollo de una Europa segura a través de la puesta en común de conocimientos de agentes con funciones policiales que pertenecen a los diferentes Estados Miembros de la UE.⁸⁶⁴ El intercambio conocimientos y la formación se focaliza en los asuntos de prioridad de la Unión en el ámbito de la seguridad, como el terrorismo y otras formas de delincuencia grave y organizada. La formación contempla actividades con asistencia a la sede de CEPOL en Budapest y actividades de aprendizaje electrónico (como seminarios web, módulos en línea, cursos en línea, etc.). También existe el fomento a los programas de intercambio entre los EEMM, el planteamiento de planes de estudio comunes en los cuerpos policiales nacionales, y el desarrollo de investigación y ciencia común en el ámbito de la seguridad.

La dirección de CEPOL recae en un director ejecutivo quien depende del Consejo de Administración. El Consejo de Administración está compuesto por representantes de los EEMM y la Comisión Europea.

⁸⁶² Decisión 2005/681/JAI del Consejo, de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI.

⁸⁶³ Reglamento (UE) n.º 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

⁸⁶⁴ En ocasiones puntuales se realiza también este ejercicio de intercambio de conocimientos con miembros policiales de terceros Estados.

Datos de contacto:

European Union Agency for Law Enforcement Training.
1066 Budapest, Ó utca 27, Hungary
E-mail: info@cepol.europa.eu
Telephone: +36 1 803 8030/8031
Fax: +36 1 803 8032

CoE (CONSEJO DE EUROPA)

El Consejo de Europa es un organismo ajeno a la Unión Europea, es decir, no pertenece a la Organización Internacional, aunque sí posee una gran importancia para los intereses de la región. La Unión Europea a menudo cuenta con la colaboración del Consejo de Europa en muchos asuntos de índole europeísta. El Consejo de Europa es la principal organización del continente europeo dedicada a la protección de los derechos humanos. La integran 46 EEMM, 27 de los cuales son miembros de la Unión Europea.

El Consejo de Europa (CoE), según sus propias declaraciones⁸⁶⁵, promueve la libertad de expresión y de los medios de comunicación, la libertad de reunión, la igualdad y la protección de las minorías. También promueve la existencia de una ciudadanía democrática, fomenta la participación de los jóvenes, la existencia de integridad en el deporte, la cultura y el patrimonio cultural y natural de Europa.

El cometido principal del CoE es establecer normas, supervisar su cumplimiento y cooperar con los Estados Miembros para combatir todo tipo de violencia o vulneración de derechos humanos en la región. Por ello centra especial atención en luchar contra la violencia machista, el abuso sexual infantil, la corrupción, los delitos cibernéticos, la discriminación, el racismo, la trata de personas, el blanqueo de capitales, el tráfico de órganos, el terrorismo y la tortura, y realiza estas acciones a la vez que defiende a la sociedad civil y protege de forma equilibrada la libertad de expresión, la libertad de prensa, las elecciones libres, la privacidad, los derechos sociales, las minorías nacionales y las lenguas minoritarias.

El CoE se encarga de proteger todos estos derechos fundamentales por medio de la celebración de convenios internacionales, así también como mediante campañas informativas, educativas y de prevención sobre una gran variedad de asuntos muy como, por ejemplo, la protección de la infancia, los discursos de odio en Internet, o los derechos del pueblo gitano, debido a que este último constituye la minoría más importante de Europa.

En términos generales el Consejo de Europa funge como un organismo de mantenimiento de paz en la región.

En el marco de los crímenes de especial gravedad, el CoE actúa de forma contundente apoyando la lucha que llevan adelante las instituciones y agencias de la Unión Europea. El Consejo de Europa ayuda a los Estados Miembros a luchar contra el terrorismo, y a emprender reformas judiciales. Su grupo de expertos constitucionales, conocido como la Comisión de Venecia, presta asesoramiento jurídico a los países a escala mundial.

Con relación al terrorismo, el Consejo de Europa desarrolló tempranamente normativa sobre el uso de Internet con finalidad terrorista al redactar el Convenio sobre la Ciberdelincuencia,⁸⁶⁶ un

⁸⁶⁵ Consejo de Europa. <https://www.coe.int/es/web/about-us/who-we-are> [Fecha de consulta: 22 de noviembre de 2023].

⁸⁶⁶ CONSEJO DE EUROPA (2001), opus cit.

instrumento centrado en la lucha contra el terrorismo y otras formas de delincuencia en Internet. Este Convenio ha sido y continúa siendo de gran referencia en la lucha contra este fenómeno. El CoE, fiel a su identidad institucional de pensar en desafíos y problemas futuros, se encuentra al presente indagando e investigando en inteligencia artificial, la bioética y el medioambiente. La estructura del Consejo de Europa está integrada por la Secretaría General, que se encarga de la dirección y de la gestión estratégica de la organización; por el Comité de Ministros, el principal órgano de toma de decisiones; la Asamblea Parlamentaria, que es el foro democrático entre diputados nacionales encargado de supervisar y debatir; el Congreso de Poder Locales y Regionales, que fomenta la democracia local y regional; el Tribunal Europeo de Derechos Humanos, quien decide sobre demandas individuales o estatales; el Comisario para los Derechos Humanos, quien promueve el respeto a los derechos humanos en los Estados Miembros; y los Órganos consultivos y de control, que son aquellos que aconsejan a los Estados Miembros y comprueban que estos respeten sus compromisos.

Datos de contacto:

Council of Europe.
Avenue de l'Europe F-67075 Strasbourg Cedex, France
E-mail: infopoint@coe.int.
Telephone: +33 (0)3 88 41 20 00
Fax: +33 (0)3 88 41 20 00

CONSEJO DE LA UNIÓN EUROPEA

El Consejo de la Unión Europea, conocido informalmente como “el Consejo” representa desde la principal instancia decisoria de la Unión y representa a todos los Estados Miembros. Está institución se creó en 1958 y su función principal es representar a los Gobiernos de los Estados Miembros, adoptar la legislación europea y coordinar las políticas de la UE. Junto con el Parlamento Europeo, el Consejo es el principal órgano decisorio de la UE.

En el Consejo de la UE, los ministros de cada Estado de la UE se reúnen para debatir, modificar y adoptar medidas legislativas y coordinar políticas, que luego resultarán en compromisos para cada gobierno nacional. A estas reuniones no hay miembros fijos, dado que asisten los ministros en funciones de cada materia que se trate. Las sesiones se realizan por asuntos a tratar y en ellas participan los ministros competentes de cada área. Los asuntos por tratar en cada área se dividen en: Asuntos Generales; Asuntos Exteriores; Asuntos Económicos y Financieros; Justicia y Asuntos de Interior; Empleo, Política Social, Salud y Consumidores; Competitividad; Transporte, Telecomunicaciones y Energía; Agricultura y Pesca; Medio Ambiente; Educación, Juventud y Cultura. Estas sesiones del Consejo a la que asisten los ministros nacionales se celebran en Bruselas, excepto durante tres meses (abril, junio y octubre), cuando se celebran en Luxemburgo.

En materia de seguridad, el Consejo constituye la institución principal para tomar decisiones en materia de Política Exterior y de Seguridad Común (PESC). En este sentido, el Consejo desarrolla la política exterior y de seguridad, siguiendo las directrices del Consejo Europeo.

Además, junto con el Parlamento, las funciones legislativas y presupuestarias. Es decir, negocia y adopta la legislación de la UE, junto con el Parlamento Europeo, a partir de las propuestas de la Comisión Europea. También, junto al Parlamento, aprueba el presupuesto anual de la UE, por

lo que tiene injerencia en el presupuesto de la Unión destinado a seguridad y defensa, conforme a las orientaciones de la CARD, coordina y orientando las políticas presupuestarias de los Estados Miembros en materia de defensa.

Finalmente, el Consejo posee la capacidad de celebrar acuerdos interinstitucionales dentro de la UE que permitan la consecución de objetivos comunes, así como acuerdos con terceros Estados y con Organizaciones Internacionales, lo que se traduce en el ámbito de la seguridad europea en una gran capacidad decisoria y de ejecución en esta materia.

La Presidencia del Consejo es ejercida por grupos de tres EEMM por un período total de dieciocho meses. Durante ese tiempo, cada Estado Miembro ejerce la Presidencia de todas las áreas por turnos de seis meses, a excepción del área de Asuntos Exteriores, presidida por el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad.

Datos de contacto:

Council of the European Union.

Rue de la Loi/Wetstraat 175

B-1048 Bruxelles/Brussel

Belgique/België

Contact form: <https://www.consilium.europa.eu/es/contact/general-enquiries/>

Telephone: +32 22816111

Fax: + 32 22816934

CONSEJO EUROPEO

El Consejo Europeo es la institución que define la orientación política y las prioridades de la Unión Europea. Estas prioridades políticas se establecen, de acuerdo con lo expresado por el propio Consejo en su sitio web,⁸⁶⁷ mediante la adopción de Conclusiones en el curso de cada sesión del Consejo Europeo. Estas Conclusiones definen asuntos específicos de interés para la UE y exponen actuaciones concretas que se han de emprender u objetivos que se han de alcanzar. Las Conclusiones del Consejo Europeo pueden asimismo fijar un plazo para alcanzar un acuerdo sobre un punto específico o para la presentación de una propuesta legislativa. De este modo, el Consejo Europeo está en condiciones de influir en la agenda política de la UE y de darle orientación.

El Consejo Europeo está compuesto por los jefes/as de Estado o de Gobierno de los 27 Estados Miembros de la UE, el/la presidente del Consejo Europeo y el/la presidente de la Comisión Europea. Este grupo en conjunto es quien planifica las políticas de la Unión y su orientación.

El Consejo Europeo es una de las siete instituciones de la UE.⁸⁶⁸ No obstante, no se trata de un órgano legislador, por lo que ni negocia ni adopta la legislación de la UE. Su cometido principal consiste más bien en determinar la dirección política general y las prioridades de la UE, fundamentalmente mediante la fijación de la agenda política de la UE.

⁸⁶⁷ Fijación de las prioridades políticas de la UE. Disponible en: <https://www.consilium.europa.eu/es/european-council/role-setting-eu-political-agenda/> [Fecha de consulta: 22 de noviembre de 2023].

⁸⁶⁸ Las instituciones de la Unión Europea son: el Parlamento Europeo (Bruselas/Estrasburgo/Luxemburgo); el Consejo Europeo (Bruselas); el Consejo de la Unión Europea (Bruselas/Luxemburgo); la Comisión Europea (Bruselas/Luxemburgo/Representaciones en los Estados Miembros), el Tribunal de Justicia de la Unión Europea (Luxemburgo); el Banco Central Europeo (Fráncfort); y, el Tribunal de Cuentas Europeo (Luxemburgo).

El Consejo Europeo establece una agenda de acción con un periodo de vigencia de cinco años. La Agenda Estratégica 2019-2024 del Consejo Europeo se centra en cuatro prioridades. La primera de estas prioridades (“proteger a los ciudadanos y las libertades”) se orienta a la seguridad.⁸⁶⁹ Dentro de la prioridad denominada a “Proteger a los ciudadanos y las libertades”, la UE determina como principio básico el establecimiento de que Europa debe de ser “un lugar en donde los ciudadanos se sientan libres y seguros.” Por ello la UE debe de defender los derechos y las libertades fundamentales de los ciudadanos europeos a fin de protegerlos contra amenazas existentes y emergentes. Teniendo esto en consideración el Consejo Europeo trabaja en las siguientes líneas de acción: el control de las fronteras exteriores de la UE; la lucha contra la migración ilegal y la trata de seres humanos mediante una mejor cooperación con los países de origen y de tránsito; el acuerdo sobre una política de asilo eficaz; la garantía del funcionamiento adecuado de Schengen; la mejora de la cooperación y el intercambio de información para combatir el terrorismo y la delincuencia transfronteriza; el aumento de la resiliencia de la UE contra las catástrofes tanto naturales como de origen humano; y la protección de nuestras sociedades contra las actividades informáticas malintencionadas, las amenazas híbridas y la desinformación.

El Consejo Europeo se reúne, como mínimo cuatro veces al año, a los Jefes de Estado o de Gobierno de los Estados Miembros e incluye, como miembro de derecho, al Presidente de la Comisión Europea.

El papel del Consejo Europeo es impulsar el desarrollo de la Unión Europea y otorgar orientación a las políticas generales. Sí bien no ejerce ninguna función legislativa, los Tratados contemplan la posibilidad de que se pronuncie en materia penal⁸⁷⁰, en caso de que algún Estado se oponga a una propuesta legislativa en este ámbito. Todas las reuniones del Consejo Europeo se celebran en Bruselas, donde también se encuentra la sede del Consejo de la Unión Europea.

Datos de contacto:

European Council.
Rue de la Loi/Wetstraat 175
B-1048 Bruxelles/Brussel
Belgique/België
Contact form: <https://www.consilium.europa.eu/es/contact/general-enquiries/>
Telephone: +32 22816111
Fax: + 32 22816934

ECTC (CENTRO EUROPEO CONTRA EL TERRORISMO)

El Centro Europeo Contra el Terrorismo (ECTC) es un centro de información especializado en terrorismo que se creó a consecuencia de varios atentados que el terrorismo yihadista realizó en Europa en el año 2015⁸⁷¹.

El ECTC es el máximo exponente de la cooperación europea contra el terrorismo y representa el primer centro de este tipo que se crea en el marco de la Política Criminal de seguridad

⁸⁶⁹ Las otras tres prioridades son: desarrollar una base económica sólida y dinámica; construir una Europa climáticamente neutra, ecológica, justa y social; y promover los intereses y valores europeos en la escena mundial.

⁸⁷⁰ También en materia de seguridad social.

⁸⁷¹ Atentados de París, 13 noviembre de 2015.

antiterrorista de la UE. Este centro, desarrollado dentro de EUROPOL, nace con el objetivo de combatir el terrorismo de una manera más eficaz.

El ECTC funciona como un centro de información de Europol para la lucha contra el terrorismo, su principal tarea es proporcionar apoyo operativo personalizado a las autoridades antiterroristas de los EEMM de la UE. Para cumplir esta tarea, el ECTC ha desarrollado su labor en cuatro pilares: Facilitación del intercambio de información y la cooperación transfronteriza; Apoyo operativo, coordinación y experiencia eficaces para las investigaciones de los Estados Miembros de la UE; Mitigación proactiva del uso de las redes sociales con fines de radicalización y apoyo al análisis operativo en investigaciones en línea; y Capacidad central de apoyo estratégico. En síntesis, el ECTC se encarga de administrar un flujo de información centralizada, reforzada y coordinada que provee y recibe de los Estados Miembros, de otros centros y unidades de EUROPOL y también de socios internacionales relevantes como INTERPOL.

El ECTC compara nuevos datos obtenidos de sus investigaciones en curso, con los datos que Europol ya tiene registrados, a fin de analizar en extenso toda la información disponible para ayudar a compilar una imagen estructurada de la red terrorista que se esté investigando en un momento concreto. El fruto de estos análisis y dicho esfuerzo permite que cada año, la ECTC publique el Informe sobre la Situación y Tendencias del Terrorismo en la UE (TE-SAT)⁸⁷², un informe de situación completo, en el que se detalla la situación del terrorismo, incluidas cifras sobre ataques terroristas y detenciones realizadas en la UE en el último año. El informe TE-SAT proporciona la experiencia y los conocimientos del ECTC en todas las áreas de los fenómenos terroristas y tiene como objetivo brindar una respuesta integral anual a la amenaza en constante cambio que supone el terrorismo en la Unión Europea.

El ECTC cuenta con un personal de más de 80 integrantes y con más de una docena de expertos nacionales en comisión de servicio. Estos miembros se distribuyen en las unidades internas que posee el ECTC. Estas son: la Unidad de Gestión de Conocimientos y Grupos de Interés (*Expertise and Stakeholder Management Unit*) proporciona apoyo estratégico central para identificar las implicaciones de la lucha contra el terrorismo en toda Europa y promover la divulgación con socios internacionales relevantes; el Equipo CBRN y Explosivos (*CBRN & Explosives Team*) es una unidad que apoya a los EEMM de la UE en el riesgo que implica el uso terrorista de las sustancias y explosivos químicos, biológicos, radiológicos y nucleares (CBRN-E), y orienta en métodos operativos de intervención; la Unidad de Operaciones (*Operations Unit*) posee especialistas y analistas que están disponibles para brindar análisis operativos para respaldar las investigaciones realizadas por las autoridades competentes de los Estados Miembros de la UE y los socios no pertenecientes a la UE; la Unidad de Referencia de Internet de la UE (*EU Internet Referral Unit*), conocida como EU IRU, coordina los esfuerzos de la UE para abordar el acceso a la propaganda terrorista en línea y brinda apoyo operativo en línea para casos de lucha contra el terrorismo; y, la Red ATLAS de Unidades de Intervención Especial⁸⁷³ (*ATLAS Network of Special Intervention Units*) que persigue el establecimiento de vínculos entre ATLAS y las comunidades antiterroristas y de delincuencia organizada y grave de Europol, y facilita el intercambio de conocimientos y prácticas estratégicas y operativas.

⁸⁷² EU Terrorism Situation & Trend Report (TE-SAT). Disponible en: <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> [Fecha de consulta: 22 de noviembre de 2023].

⁸⁷³ La Red ATLAS es una asociación europea de las unidades especiales de policía de los EEMM de la UE, que se enfoca en cooperar en la lucha contra el terrorismo y la delincuencia organizada. La red es financiada por la Comisión Europea, a través de su Dirección General de Asuntos de Interior. La Red ha sido creada en 2001 y surgió como una organización informal tras los atentados del 11 de septiembre de 2001. Desde el 2019 la red Atlas se ha afiliado a Europol, en donde posee la sede.

Datos de contacto:

European Counter Terrorism Centre.
Eisenhowerlaan 73
2517 KK The Hague, The Netherlands
Postal address: P.O. Box 908 50 2509 LW The Hague, The Netherlands
Telephone: +31 70 302 5000
Press and journalists: + 31 70 302 5001

EDA (AGENCIA EUROPEA DE DEFENSA)

La Agencia Europea de Defensa (EDA) es una agencia descentralizada de la Unión Europea que fue creada en el año 2004. La función de la EDA consiste en ayudar a sus veintisiete Estados Miembros de la UE a mejorar las capacidades de defensa y sus recursos militares, por medio de la cooperación europea.

La EDA desempeña un papel fundamental al promover el desarrollo de la Política Común de Seguridad y Defensa (PCSD) de la UE. Fomenta la colaboración, introduce nuevas iniciativas y aporta soluciones para mejorar la capacidad defensiva conjunta de la UE y de sus EEMM.

La EDA ostenta una plantilla de aproximadamente ciento ochenta personas, y actualmente está dirigida por Josep Borrell, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad y vicepresidente de la Comisión Europea.

En esta agencia se desarrolla una gran variedad de actividades del ámbito de la defensa, entre ellas: armonización de los requisitos para la consecución de capacidades operativas; investigación e innovación para el desarrollo de demostradores tecnológicos; formación y ejercicios de mantenimiento en apoyo de las operaciones de Política Común de Seguridad y Defensa (PCSD). La EDA trabaja también para fortalecer la industria de la defensa europea y actúa como facilitador e intermediario entre las partes interesadas del ámbito militar de los EEMM y las políticas de la UE que inciden en la defensa.

En mayo de 2017, los Estados Miembros acordaron reforzar la misión de la Agencia, convirtiéndola en el operador central de las actividades relacionadas con la defensa financiadas por la UE.

Datos de contacto:

European Defense Agency.
Rue des Drapiers/Lakenweversstraat 17-23
1050 Bruxelles/Brussel
Belgique/België
Telephone: +32 25042800
Fax: +32 25042815

EEMM (ESTADO/S MIEMBRO/S)

Los Estados Miembros de la Unión Europea son los 27 países soberanos que forman parte de la Organización Internacional. Estos son, Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia,

Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, Rumania y Suecia, entre los cuales se contabiliza veintiún repúblicas y seis monarquías.

Todos los Estados Miembros son partes de los Tratados de la Unión Europea (TUE), que son el Tratado de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea (TFUE). Los EEMM de la UE se encuentran vinculados entre sí por el compromiso político, económico y jurídico que deriva del proceso de integración europea asumido por todos en el marco de estos tratados constitutivos mencionados. El TUE y el TFUE establecen que todos los Estados Miembros son soberanos y poseen igual valor dentro de la UE, este hecho resulta fundamental dado que los Estados delegan soberanía a cambio de representación en las instituciones europeas.

Las instituciones de la Unión Europea poseen la facultad de dictar leyes y ejecutarlas en el dentro del espacio comunitario. Si un Estado incurre en incumplimiento de una ley de la UE, este puede ser multado o se le pueden retirar fondos. En casos extremos, limitar el derecho a voto o suspender la pertenencia de un Estado Miembro.

El alto nivel de integración europea ha permitido que la UE posea relativa interferencia en los asuntos internos de cada Estado, excepto en los asuntos relativos a defensa, seguridad y política exterior en donde todas los temas de prioridad europea en este ámbito se dirimen por medio de la cooperación y unanimidad. Es aquí en donde se prioriza la armonización a fin de dar consecución a las prioridades de la UE en materia de seguridad, defensa y política exterior. Ello significa, la aproximación máxima de las legislaciones de Derecho penal interno y de medidas policiales y judiciales que permitan una colaboración horizontal y vertical⁸⁷⁴reciproca y equilibrada.

ENISA (AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD)

ENISA (Agencia de la Unión Europea para la Ciberseguridad) es la agencia de la Unión Europea que posee la misión de velar por un alto nivel común de ciberseguridad en toda Europa. Ha sido creada en el año 2004, bajo el mandato y marco regulatorio del Reglamento sobre la Ciberseguridad de la UE.⁸⁷⁵

De acuerdo con sus propias palabras,⁸⁷⁶ contribuye al desarrollo de una política de seguridad cibernética de la UE, busca incrementar la fiabilidad de los productos, servicios y procesos de Tecnologías de la Información y Comunicación (TIC), fomenta la cooperación con los EEMM y con instituciones y agencias de la UE, y promueve la existencia de una región europea preparada a nuevos desafíos de ciberseguridad. La Agencia coopera con las principales partes interesadas mediante el intercambio de información y conocimientos, el aumento de la resiliencia de las infraestructuras de la Unión y, por medio de la protección de la sociedad y

⁸⁷⁴ Cooperación vertical es la que tiene lugar entre la Unión Europea y los Estados Miembros. Cooperación horizontal es la que se da entre los Estados Miembros de la UE entre sí.

⁸⁷⁵ Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad).

⁸⁷⁶ Agencia de la Unión Europea para la Ciberseguridad. Disponible en: <https://www.enisa.europa.eu/about-enisa/about/es> [Fecha de consulta: 22 de noviembre de 2023].

ciudadanía europea de las amenazas digitales. La labor de ENISA es fundamental en la actualidad dado que el mundo se encuentra sumido en la hiperconectividad, y ello induce a que este expuesto a múltiples vulnerabilidades cibernéticas. Por la naturaleza global de Internet, ciberataques no poseen fronteras, por tanto, afectan a más de un Estado y a todas las capas de la sociedad. La Unión Europea se prepara con ENISA para responder a las crisis cibernéticas y a los ciberataques masivos, mediante una respuesta rápida y coordinada a nivel estratégico, operativo, técnico y comunicativo. Para ello, ENISA dispone desde el 27 de junio de 2019, de la Red Nacional de Oficiales de Enlace (*National Liaison Officers Network, o NLO Network*), cuya función es facilitar el intercambio de información entre ENISA y los EEMM de la UE. La Red NLO desempeña un papel fundamental en la implementación del programa de trabajo anual de ENISA al identificar a los grupos interesados en apoyar el trabajo de ENISA, y al informar acerca de los desarrollos nacionales en materia de ciberseguridad y apoyar en la difusión de actividades, hallazgos y recomendaciones de cada EEMM.

ENISA también promueve la cooperación con socios en externos a la Unión Europea. En enero del año 2023 la Agencia de Ciberseguridad de la Unión Europea (ENISA) ha firmado un acuerdo de trabajo con la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EEUU, para promover el desarrollo conjunto de capacidades, de mejores prácticas y de la conciencia situacional.⁸⁷⁷ Los primeros resultados de este acuerdo se darán a conocer en el Diálogo Cibernético UE-EEUU, previsto para la segunda mitad de 2023.

Datos de contacto:

European Union Agency for Cybersecurity.
Ethnikis Antistaseos 72 & Agamemnonos 14
Chalandri 15231, Attiki, Greece
E-mail: info@enisa.europa.eu
Telephone: +30 28 14 40 9711
Fax: +30 28 14 40 9711

EU INTCEN (CENTRO DE INTELIGENCIA Y SITUACIÓN DE LA UE)

El Centro de Inteligencia y Situación de la UE (EU INTCEN) es un centro de análisis que procesa toda la información que se recibe por cualquier medio y de cualquier fuente legitimada, incluidos los servicios nacionales de información de los Estados Miembros.

La misión de EU INTCEN es proporcionar análisis de inteligencia, alerta temprana y conocimiento de la situación al Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (AR) y al Servicio Europeo de Acción Exterior (SEAE).

A su nacimiento, en el año 2002, esta red fue conocida con el nombre de SITCEN, y desde sus comienzos ha permitido compartir información entre los EEMM, y gestionar información e investigaciones junto a EUROPOL. No obstante, se trataba de una estructura que trabajaba exclusivamente en inteligencia de fuente abierta (OSINT).

EU SITCEN ha sido creada para que la Unión Europea contase con una red propia y cerrada de inteligencia. La Unión Europea ha asumido tempranamente que no se le podía pedir a los

⁸⁷⁷ Joint Statement by United States Secretary of Homeland Security Mayorkas and European Union Commissioner for Internal Market Breton. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_394 [Fecha de consulta: 22 de noviembre de 2023].

servicios nacionales de inteligencia que compartan información en una red abierta, obtenida por sus propios medios y esfuerzo, con otros 26 EEMM. El no contar por lo tanto con información proveniente de servicios de inteligencia, dejaba en un gran escenario de vulnerabilidad a la Unión al funcionar “a ciegas” en el Sistema internacional. Debido a ello se creó una red de servicios de inteligencia exclusiva de la Unión Europea a fin de orientar al Alto Representante (AR) en su gestión y a los EEMM.

El centro fue originariamente formado por expertos de los servicios exteriores de la UE. Ello ha sido así porque inicialmente EU SITCEN fue concebido para evaluar crisis internacionales. Años más tarde comenzó a proveer información tendiente a reforzar la seguridad interior y la lucha contra el terrorismo, incorporando variedad de especialistas de servicios de inteligencia que han ido paulatinamente incrementándose en función de la propia ampliación de la Unión Europea.

En 2005, el SITCEN de la UE se vio reforzado con la llegada de un equipo de expertos antiterroristas adscritos por los servicios de seguridad de los Estados Miembros. Esto permitió a SITCEN proporcionar al Consejo de la Unión Europea evaluaciones estratégicas de amenazas terroristas basadas en información de inteligencia de los servicios nacionales.

En el año 2007 se produce un refuerzo de este centro y EU SITCEN pasa a formar parte de la Capacidad Única de Análisis de Inteligencia (*Single Intelligence Analysis Capacity*, SIAC)⁸⁷⁸, que combina la inteligencia civil (EU SITCEN) y la inteligencia militar (*European Union Military Staff*, EUMS⁸⁷⁹). En este marco de acción conjunta, se utilizan contribuciones tanto civiles como militares para producir análisis de inteligencia de todas las fuentes, alertas tempranas y conciencia situacional.

Con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009, EU SITCEN quedó bajo la autoridad del Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad/Vicepresidente de la Comisión. El 1 de enero de 2011, el EU SITCEN fue transferido al Servicio Europeo de Acción Exterior (SEAE).

En marzo de 2012, pasó a llamarse oficialmente Centro de Análisis de Inteligencia de la Unión Europea. Finalmente asumió su nombre actual, Centro de Inteligencia y Situación de la UE (*EU Intelligence and Situation Centre*, EU INTCEN) en el año 2015.

Las funciones actuales de EU INTCEN son: proporcionar información exclusiva que no esté disponible abiertamente ni se haya proporcionado en otro lugar al Alto Representante/Vicepresidente (AR/VP) y al Comité Político y de Seguridad de la Unión Europea (*Political and Security Committee*, PSC), basándose en las contribuciones de los servicios de inteligencia y seguridad de los Estados Miembros; Proporcionar evaluaciones e informes y una gama de productos basados en inteligencia y fuentes abiertas al Alto Representante/Vicepresidente (AR/VP) y al SEAE, a los diversos órganos de toma de decisiones de la UE en los campos de la PESC y la PCSD, así como a los Estados Miembros; Actuar como punto de entrada único en la UE para información clasificada procedente de los servicios civiles de inteligencia y seguridad de los Estados Miembros; y, Apoyar y asistir al Presidente del

⁸⁷⁸ SIAC proporciona aportaciones de inteligencia para la alerta temprana y evaluación de la situación, así como aportaciones de inteligencia para la planificación y evaluación de la respuesta a crisis en el teatro de operaciones y ejercicios. Todas las evaluaciones de inteligencia enviadas a los Estados Miembros son productos conjuntos preparados en el marco de la SIAC.

⁸⁷⁹ El Estado Mayor de la Unión Europea (EUMS) posee la función principal de brindar experiencia militar y apoyo a la PCSD, incluido el planeamiento y conducción de operaciones militares de gestión de crisis dirigidas por la UE. El EUMS evolucionó paralelamente al nivel de especialización de la UE en el ámbito de la PESC y la PCSD. Orgánicamente al inicio dependía de la Secretaría General del Consejo. Actualmente depende orgánicamente del Servicio Europeo de Acción Exterior (SEAE), creado en el año 2011.

Consejo Europeo y al Presidente de la Comisión Europea en el ejercicio de sus respectivas funciones en el ámbito de las relaciones exteriores.

EU INTCEN monitorea y evalúa eventos internacionales las 24 horas del día, los 7 días de la semana, centrándose particularmente en áreas geográficas sensibles, y eventos de terrorismo y otras amenazas globales.

EU IRU (UNIDAD DE REFERENCIA DE LA UNIÓN EUROPEA)

La Unidad de Referencia de Internet (EU IRU) es una unidad operativa creada dentro del Centro Europeo de Lucha contra el Terrorismo (ECTC) de Europol en el año 2015. La función de la Unidad de Referencia de Internet (EU IRU) es rastrear, alertar e investigar las acciones criminales que realiza el terrorismo en Internet, así también como detectar todo tipo de contenido violento extremista en la red, ya sea páginas webs o redes sociales.

LA EU IRU es la unidad más importante que hemos de analizar en el desarrollo de este estudio sobre la Política Criminal de la UE con relación al terrorismo yihadista en Internet. Debido a ello, se le ha brindado en esta investigación un segmento preferente de análisis dentro del propio cuerpo del texto.⁸⁸⁰

Datos de contacto:

EU Internet Referral Unit.
Eisenhowerlaan 73
2517 KK The Hague, The Netherlands
Postal address: P.O. Box 908 50 2509 LW The Hague, The Netherlands
Telephone: +31 70 302 5000
Press and journalists: + 31 70 302 5001

EUROJUST (AGENCIA DE LA UNIÓN EUROPEA PARA LA COOPERACIÓN JUDICIAL PENAL)

Eurojust, la Agencia de la Unión Europea para la Cooperación en materia de Justicia Penal, es una agencia de la Unión Europea en donde las autoridades judiciales nacionales de los EEMM de la Unión trabajan de forma estrecha y colaborativa para luchar contra la delincuencia transfronteriza organizada grave.

La agencia Eurojust fue creada en el año 2002⁸⁸¹ y está compuesto por 27 fiscales o jueces nombrados por cada EEMM de la UE. Todos estos miembros nacionales deben tener una experiencia y trayectoria acreditada para el cargo por desempeñar.

La función de Eurojust es crear en Europa una zona más segura coordinando para ello el trabajo de las autoridades nacionales (tanto de los Estados Miembros de la UE como de terceros Estados) en la investigación y el procesamiento de la delincuencia transnacional.

⁸⁸⁰ Ver: “MEDIDAS DE VIGILANCIA Y CONTROL DE INTERNET” EN EL CAPÍTULO 6: MEDIDAS INSTITUCIONALES DE LA UNIÓN EUROPEA TENDIENTES A LA COOPERACIÓN EN EL CONTROL Y VIGILANCIA DE INTERNET Y A LA REPRESIÓN SOBRE SU USO CON FINES YIHADISTAS.

⁸⁸¹ Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

Eurojust tiene como objetivo la promoción del trabajo coordinado entre las autoridades competentes de los EEMM, así como brindar asistencia judicial internacional y asistir en la ejecución de solicitudes de extradición o la orden europea de detención y entrega.

Eurojust asiste a los EEMM de la UE en la lucha contra el terrorismo y otras formas graves de delincuencia organizada ofreciendo los servicios de: coordinación en investigaciones y enjuiciamientos que afecten como mínimo a dos Estados; ayuda para dirimir conflictos de jurisdicción; elaboración y aplicación de instrumentos jurídicos de la UE.

También colabora con investigaciones de carácter penal iniciadas por los EEMM sobre la base de análisis realizados por Europol. Desde el año 2004, a raíz de un acuerdo de colaboración entre ambas agencias, Eurojust y Europol, trabajan conjuntamente, entre otros, en asuntos de delincuencia informática y la participación en organización terrorista o delictiva.

El trabajo de Eurojust se materializa en las denominadas Reuniones de Coordinación, cuya finalidad poner en contacto entre sí a investigadores y autoridades judiciales de los EEMM.

Durante estas reuniones se toman decisiones de carácter ejecutorio y operativo como determinación de día y lugar de detenciones, los registros domiciliarios, ejecución de una Euroorden, etc., y otras medidas orientadas a los grupos criminales que operan en la UE.

Además, realiza equipos conjuntos de investigación, en donde jueces de instrucción, fiscales y funcionarios policiales de diferentes EEMM colaboran en la lucha contra el terrorismo y otras formas de delincuencia organizada.

En un marco extracomunitario, Eurojust ha firmado acuerdos de cooperación con terceros Estados (Croacia, EEUU, Islandia, Noruega y Suiza), y los fiscales de enlace de tres de ellos, Noruega, EEUU y Croacia, tienen base permanente en Eurojust. En el año 2009 se han adoptado medidas legislativas⁸⁸² para mejorar la eficacia de la cooperación judicial de Eurojust.

Datos de contacto:

European Union Agency for Criminal Justice Cooperation.

Johan de Wittlaan 9

2517 JR The Hague

Netherlands

E-mail: info@eurojust.europa.eu

Telephone: +31 70 412 5000

Fax: +31 70 412 5005

EUROPOL (AGENCIA DE LA UNIÓN EUROPEA PARA LA COOPERACIÓN POLICIAL)

La creación de Europol (Agencia de la Unión Europea para la Cooperación Policial, - ex Oficina Europea de Policía-) ha supuesto uno de los mayores progresos realizados en el marco de la seguridad europea. Sí bien se creó en abril de 2009 por mandato del Consejo⁸⁸³, recién a partir del 1 de enero de 2010 se convirtió en una agencia oficial de la Unión Europea.

⁸⁸² Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008 por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

⁸⁸³ Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (EUROPOL)

Europol no es una policía europea⁸⁸⁴, sino un órgano de cooperación entre los servicios de policía y aduanas de cada EEMM, y tiene por misión general hacer cumplir la ley en la Unión Europea.

Europol es una agencia al servicio de los Estados Miembros para cooperar en la lucha contra la delincuencia organizada transnacional y el terrorismo. Su actuación específica implica, por una parte, en facilitar la transmisión de información entre los servicios nacionales entre sí (facilitar la cooperación horizontal entre los EEMM) y, por la otra, ofrecer diversos análisis sobre delincuencia organizada transnacional y terrorismo a los Estados de la Unión. Para este último caso se integra como un miembro más a los equipos de investigación formados por los servicios de los distintos EEMM, y actúa proporcionándoles sobre el terreno la información que necesiten. En términos generales la misión de Europol es brindar apoyo a sus EEMM en la prevención y lucha contra todas las formas graves de delincuencia internacional y organizada, ciberdelincuencia y terrorismo.

Ante el incremento de los casos de terrorismo yihadista, en el año 2016 se amplían las capacidades jurídicas de Europol⁸⁸⁵ y en el año 2018, mediante la Decisión (UE) 2018/890⁸⁸⁶ designa en este caso a Europol como contacto común para el intercambio de información acerca de las personas que viajan al extranjero para recibir adiestramiento militar y posteriormente regresar a Europea con fines de realizar la yihad en territorio comunitario. El Reglamento (UE) 2016/794 y Decisión (UE) 2018/890 permiten a Europol intensificar sus esfuerzos en la lucha contra el terrorismo, la ciberdelincuencia y otras formas graves y organizadas de delincuencia transnacional. El reglamento, además, refuerza la capacidad de Europol para fomentar la cooperación interna entre las autoridades nacionales encargadas de hacer cumplir la ley en la UE. Europol solidifica así un trabajo con un gran enfoque interinstitucional e internacional, fomentando la cooperación interinstitucional con otras agencias e instituciones de la UE, y en el ámbito internacional cooperando con diversos Estados, hacia dentro y hacia fuera de la Unión. La decisión sobre qué delitos priorizar en este contexto de alta demanda está determinada por EMPACT⁸⁸⁷

Según Europol, las mayores amenazas a la seguridad provienen de: el terrorismo; el tráfico internacional de drogas y lavado de dinero; el fraude organizado; la falsificación de euros; y, el tráfico de seres humanos. Con relación al terrorismo, Europol trabaja con varias líneas de acción. TE-SAT: es un informe sobre la situación y tendencias del terrorismo en la UE que Europol elabora cada año desde 2007, y que ofrece una visión general de los ataques fallidos, frustrados y consumados en la UE, así como de las detenciones, condenas y sanciones relacionadas con el terrorismo. Sí bien TE-SAT contabiliza varias formas de terrorismo, identifica que la tendencia del terrorismo en los informes de los últimos años es hacia el terrorismo yihadista.

⁸⁸⁴ Los agentes de Europol nunca arrestan a ciudadanos ni inician investigaciones. Su competencia está limitada a ser un organismo de cooperación y apoyo para los servicios policiales nacionales de los EEMM.

⁸⁸⁵ Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial.

⁸⁸⁶ Decisión (UE) 2018/890 relativa a la celebración, en nombre de la Unión Europea, del Protocolo Adicional al Convenio del Consejo de Europa para la prevención del terrorismo.

⁸⁸⁷ EMPACT es una herramienta metodológica introducida entre los años 2012 y 2013 para luchar de forma multidisciplinaria y multiinstitucional contra formas graves de delincuencia. Significa Plataforma Multidisciplinaria Europea Contra las Amenazas Criminales (*European Multidisciplinary Platform Against Criminal Threats*). Introduce un enfoque integrado de la seguridad interior de la UE, que incluye medidas que van desde los controles de las fronteras exteriores, la cooperación policial, aduanera y judicial hasta la gestión de la información, la innovación, la formación, la prevención y la dimensión exterior de la seguridad interior, así como asociaciones público-privadas.

EC3: es el Centro Europeo de Ciberdelincuencia comenzó a funcionar dentro de Europol en el año 2013. Coordina las policías nacionales de la UE para combatir contra los delitos transnacionales cometidos por medio de Internet. Dentro de EC3 funciona desde el 2014 el Grupo de Trabajo Conjunto de Acción contra la Ciberdelincuencia (J-CAT), que ayuda a luchar contra la ciberdelincuencia dentro y fuera de la UE.

EU IRU: se crea en el año 2015 y se encarga de la identificación y la eliminación de publicaciones con contenido del terrorismo yihadista en Internet.

ECTC: en enero de 2016 se crea dentro de Europol el Centro Europeo Contra el Terrorismo, para mejorar la cooperación transfronteriza entre las autoridades antiterroristas de los EEMM.

Europol también trabaja con muchos estados socios no pertenecientes a la UE y Organizaciones Internacionales. Entre ellas, muchas de terceros Estados, principalmente EEUU, como: Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos (*Bureau of Alcohol, Tobacco, Firearms and Explosives*, ATF), Aduanas y Protección Fronteriza (*Customs and Border Protection*, CBP), Administración de Control de Drogas (*Drug Enforcement Administration*, DEA), Servicio de Seguridad Diplomática (*Diplomatic Security Service*, DSS), Oficina Federal de Investigaciones (*Federal Bureau of Investigation*, FBI), Administración de Alimentos y Medicamentos (*Food and Drug Administration*, FDA), Servicio de Inmigración y Aduanas (*Immigration and Customs Enforcement*, ICE), Servicio de Impuestos Internos (*Internal Revenue Service*, IRS), Agencias de EEUU - Tesoro de EEUU. - Red de control de delitos financieros (*US Agencies - US Treasury – Financial Enforcement Network*, FinCEN), Departamento de Policía de Nueva York (*New York Police Department*, NYPD), Servicio Secreto (*Secret Service*, USSS), y Administración de Seguridad del Transporte (*Transportation Security Administration*, TSA).

La sede de Europol se ubica en La Haya, Países Bajos. Posee más de 1400 empleados, más de 260 funcionarios de enlace, y cada año apoya a miles de investigaciones europeas e internacionales con relación al terrorismo yihadista, ciberdelincuencia y otras formas graves de delincuencia transnacional.

Datos de contacto:

European Union Agency for Law Enforcement Cooperation.

Eisenhowerlaan 73

2517 KK The Hague, The Netherlands

Postal address: P.O. Box 908 50 2509 LW The Hague, The Netherlands

Telephone: +31 70 302 5000

Press and journalists: + 31 70 302 5001

EUROSUR (SISTEMA EUROPEO DE VIGILANCIA DE FRONTERAS)

Eurosur es una red de comunicación. Este sistema paneuropeo de vigilancia fronteriza, puesto en marcha en octubre de 2013, está orientado a mejorar la eficacia en la detección, prevención y lucha contra la inmigración irregular y la delincuencia organizada. Su principal objetivo es ayudar a gestionar con eficacia las fronteras exteriores de la UE. Para ello fomenta el intercambio de información con los puestos de vigilancia nacionales de cada EEMM de la Unión y con la agencia Frontex.

Si bien Eurosur no es una institución, agencia o unidad de la Unión Europea y por ello, desde un punto de vista clasificatorio, no debería de ser incluido en este glosario, resulta de especial importancia en la lucha contra el terrorismo.

Según Erik Berglund, director encargado del refuerzo de la capacidad de Frontex, un triple objetivo: “Detectar a los inmigrantes clandestinos, luchar contra la delincuencia internacional y salvar a los refugiados que huyen en barco”. Este sistema permite rastrear y compartir en tiempo real datos protegidos recabados por distintas autoridades nacionales como imágenes de satélite, previsiones meteorológicas o sistemas de indicación de la posición de barcos. Según la información que la agencia Frontex ha obtenido mediante el uso de la red Eurosur, en el último año ha habido un incremento del 300% sobre el flujo migratorio irregular con destino a Europa.⁸⁸⁸ Este dato es especialmente relevante debido a que, en la lucha contra el terrorismo yihadista en Internet, son sujetos de especial atención aquellos que viajan a Siria o Irak y retornan a Europa para *hacer la yihad*⁸⁸⁹ en territorio comunitario.

Se insta a los EEMM que utilizan Eurosur a respetar en todo momento los derechos humanos, incluido el principio de "no devolución", que prohíbe el retorno de una persona a un lugar donde su vida o sus libertades puedan verse amenazadas, especialmente en casos en donde no existe ninguna comisión de delito ni vulneración o amenaza del territorio europeo. Tampoco se debe o puede enviar información a terceros Estados que pueda ser utilizada por estos para identificar a una persona cuya solicitud de protección internacional está siendo procesada o cuya vida o integridad física pudiese estar en peligro.

FRONTEX (AGENCIA EUROPEA DE LA GUARDIA DE FRONTERAS Y COSTAS)

La Agencia Europea de la Guardia de Fronteras y Costas (Frontex), se creó en 2004 para ayudar a los Estados Miembros de la UE y a los otros Estados asociados a Schengen a proteger las fronteras exteriores de la UE. La función de Frontex es evaluar los riesgos para la seguridad en las fronteras de la UE, y facilitar agentes policiales de los EEMM y de los países del espacio Schengen en zonas fronterizas exteriores que necesitan asistencia adicional.

Frontex supervisa 24x7 las fronteras exteriores de la Unión Europea y proporciona actualizaciones y alertas a los EEMM de la UE y los Estados del espacio Schengen, a la Comisión Europea y a otras agencias de la Unión. Informa a las autoridades policiales, agencias de la UE y aduanas en las fronteras marítimas sobre la comisión de delitos que tienen lugar en las fronteras exteriores de la Unión, como tráfico ilícito de inmigrantes, trata de seres humanos,

⁸⁸⁸ «La entrada irregular de migrantes a la UE por el Mediterráneo central alcanza máximos históricos», *El País*, edición online de 12 de mayo de 2023. Disponible en: <https://elpais.com/internacional/2023-05-12/la-entrada-irregular-de-migrantes-a-la-ue-por-el-mediterraneo-central-alcanza-maximos-historicos.html> [Fecha de consulta: 22 de noviembre de 2023].

⁸⁸⁹ Se refiere a personas que viajan al extranjero a recibir adiestramiento militar para la comisión de ataques terroristas que serán llevados a cabo a su regreso a Europa. El proceso habitual que los sujetos delictivos realizan implica varias etapas. Primero, toman contacto por medio de Internet con grupos terroristas asentados en Siria e Irak, en donde serán recibidos en los campos de entrenamiento. Segundo, efectúan el viaje de salida de Europa en avión hacia el país de destino. Generalmente en esta etapa han sido ya identificados por el uso yihadista que han realizado previamente de Internet. Tercero, debido a la identificación en el uso de Internet y la identificación de salida de territorio europeo, a su retorno a Europa suelen hacerlo por otras vías que dificulte la identificación de ingreso por parte de las autoridades policiales de los Estados de la Unión. Ello determina que habitualmente su regreso a Europa se realice por medio de la inmigración irregular. En el ámbito del terrorismo, Eurosur es una herramienta que ayuda en la detección de la última fase de este proceso al proveer a las agencias Frontex y Europol datos e información relevante en esta materia.

terrorismo⁸⁹⁰, y otras actividades delictivas transfronterizas que tienen lugar en las fronteras externas de la Unión.

Frontex posee funcionarios de enlace en los EEMM de la UE para ayudar a la agencia en la ejecución de sus funciones. La Agencia comparte la información recopilada en las fronteras con EEMM, Europol y con otras agencias y centros de análisis europeos.

Con respecto a la inmigración irregular Frontex desarrolla un trabajo fundamental en el retorno a sus países de origen de las personas que no tienen derecho a permanecer en la Unión Europea. Coordina y financia operaciones de retorno, y también asiste a los EEMM en este cometido.⁸⁹¹

Para garantizar el control externo de la fronteras europeas, Frontex ha creado una red con autoridades fronterizas de terceros Estados, en particular, con los países limítrofes a la UE, que son países de origen y tránsito de inmigrantes. En estos terceros Estados fronterizos, Frontex ha situado funcionarios de enlace a fin de tener mayor control fronterizo.

En caso de ser necesario, esta agencia posee la capacidad de desplegar rápidamente equipos y guardias de fronteras y de costas hacia las fronteras exteriores de la UE que se encuentren en una situación de emergencia. Lo hace mediante las Agrupaciones Tácticas de Reacción Rápida (*EU Battlegroups*) que proporcionan los EEMM a petición de la agencia, y permite movilizar hasta 1500 agentes donde Frontex lo requiera.

En un ámbito regulatorio de acceso a la Unión Europea por vía aérea, Frontex ayuda a construir la armonización normativa del espacio comunitario que garantice normas uniformes respecto del control de fronteras exteriores, de tal forma que, para una persona procedente de un tercer Estado, las fronteras exteriores de la Unión sean siempre igual con independencia del país desde donde quiera hacer su ingreso a Europa. Para este control, que opera en todos los Estados de la Unión, Frontex se apoya en el Sistema Europeo de Información y Autorización de Viajes (ETIAS)⁸⁹², en funcionamiento desde el año 2023. Frontex albergará la unidad central del ETIAS, que funcionará las 24 horas del día, 7 días a la semana, para tramitar las solicitudes correspondientes.

Datos de contacto:

European Border and Coast Guard Agency.
Plac Europejski 6
00-844 Warsaw, Poland
E-mail: frontex@frontex.europa.eu
Telephone: (48 22) 205 95 00
Fax: (48 22) 205 95 00

PARLAMENTO EUROPEO

El Parlamento Europeo es un importante foro de debate político y de decisión en la Unión Europea. El Parlamento posee, junto al Consejo, la responsabilidad de adoptar, modificar

⁸⁹⁰ Se refiere a terroristas yihadistas retornados a Europa que intentan ingresar al espacio comunitario de forma ilegal y no sin ser identificados.

⁸⁹¹ Se refiere a acciones concretas que Frontex puede realizar como poner a disposición vuelos chárter o reservar asientos en vuelos comerciales. Frontex facilita también los documentos de viaje para los retornados y pone a disposición de los EEMM expertos propios para ayudar en estas operaciones.

⁸⁹² ETIAS es un sistema que regula el acceso a Europa, mediante la expedición de una autorización de viaje, que deben solicitar personas que ingresan desde terceros países y que estén exentos de visa.

propuestas legislativas y decidir acerca del presupuesto y la legislación de la UE. Ambas instituciones actúan como colegisladores en pie de igualdad en el marco del procedimiento legislativo ordinario.

El Parlamento Europeo además supervisa la actividad de la Comisión y de otros órganos de la UE, y coopera con los órganos parlamentarios de los EEMM de la UE encauzando en la legislación común sus aportaciones.

Con los cambios en los Tratados europeos (TUE y TFUE), el Parlamento adquirió paulatinamente mayores poderes legislativos y presupuestarios que le permiten fijar, junto a la representación de los gobiernos de los EEMM en el Consejo, la dirección hacia la que se orienta el proyecto europeo. Los Tratados (TUE y TFUE) otorgan una gran prioridad a la creación de un espacio de libertad, seguridad y justicia, un elemento clave en la seguridad de Europa y en el ámbito de la lucha contra el terrorismo. El Título V del Tratado de Funcionamiento de la Unión Europea (TFUE) (artículos 67 a 89) está dedicado al espacio de libertad, seguridad y justicia, y además de disposiciones generales este título incluye capítulos específicos dedicados a las políticas sobre controles en las fronteras, asilo e inmigración, a la cooperación judicial en materia penal, y a la cooperación policial de los Estados Miembros. Esto es debido principalmente al hecho de que pensar en términos de “libertad, seguridad y justicia” significa adoptar medidas que aseguren dichos compromisos. Por ello el Título V del TFUE faculta al Parlamento Europeo (y Consejo) a legislar sobre los temas a los que sus artículos se refieren. El artículo 72 se refiere al fomento de la seguridad interior de la Unión. El artículo 73 a la promoción de la cooperación entre EEMM por medio de “servicios competentes de sus administraciones responsables de velar por la seguridad nacional”, es decir policías nacionales (Competencia de Europol). El artículo 75 se refiere concretamente a la adopción de reglamentos que realiza el Parlamento Europeo y el Consejo para luchar contra el terrorismo en la Unión Europea y su financiación. El artículo 77 se refiere al control de fronteras exteriores de la Unión. El artículo 78 describe la necesidad de una política común de migración (competencia de Frontex). El artículo 82 se refiere a la cooperación judicial en materia penal basada en el principio de reconocimiento mutuo de las resoluciones judiciales y extrajudiciales (Competencia de Eurojust). El artículo 83 expresa la competencia que poseen el Parlamento y el Consejo para adoptar directivas en ámbitos delictivos como el terrorismo, la trata de seres humanos y la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada.

Todos estos asuntos, y otros, relativos concretamente a la seguridad de la Unión son materia de legislación en el Parlamento Europeo. El Parlamento está compuesto por 705 parlamentarios (eurodiputados) que representan a la población europea⁸⁹³ y que son elegidos por sufragio universal en los 27 Estados Miembros de la Unión Europea. Los eurodiputados del Parlamento Europeo no se agrupan por sus respectivos EEMM de origen, sino por grupos políticos.

Datos de contacto:

European Parliament Bruxelles/Brussel.
60 rue Wiertz / Wiertzstraat 60
B-1047 - Bruxelles/Brussels
E-mail: eplobelgium@europarl.europa.eu

⁸⁹³ A la fecha 450 millones de personas aproximadamente.

Telephone: +32 (0)2 28 42111
Fax: +32 (0)2 28 42111

European Parliament Strasbourg.
Allée du Printemps
B.P. 1024 F-67070 - Strasbourg
E-mail: epstrasbourg@europarl.europa.eu
Telephone: +33 (0)3 88 1 74001
Fax: +33 (0)3 88 1 74001

European Parliament Luxembourg.
Plateau du Kirchberg
B.P. 1601 L-2929 - Luxembourg
E-mail: epluxembourg@europarl.europa.eu
Telephone: +352 4300 22333
Fax: +352 4300 22333

RJE (RED JUDICIAL EUROPEA EN MATERIA PENAL)

Creada en 1998 por Decisión del Consejo de la Unión Europea. Facilita el auxilio judicial en el marco de la lucha contra la delincuencia transnacional. La Red está constituida por puntos de contacto establecido en cada EEMM, de los cuales las autoridades judiciales de otros EEMM pueden obtener información jurídica y práctica necesaria y mantener contacto directo para cooperar.

La Red Judicial Europea (RJE) en materia penal es una red de contacto de competencias nacionales para facilitar la cooperación judicial. La RJE fue creada por Decisión del Consejo de la Unión Europea mediante la Acción Común 98/428 JAI de 29 de junio de 1998 para cumplir la recomendación n°21 del Plan de Acción para combatir la delincuencia organizada adoptado por el Consejo el 28 de abril de 1997. En el año 2008 se buscó reforzar el estatus jurídico de la RJE y se adoptó la Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea.⁸⁹⁴ La RJE está estructurada mediante puntos de contacto en cada EEMM, con un corresponsal nacional que desempeña la labor de coordinación. La función principal de estos puntos de contacto es ser intermediarios activos, y asegurar la cooperación judicial en asuntos penales entre los EEMM de la UE, particularmente en acciones para combatir formas de delitos graves, como el terrorismo o ciberterrorismo. La RJE tiene su Secretaría en Eurojust, quien es titular de su administración. La Secretaría de la RJE tiene control sobre los puntos de contacto y garantiza el funcionamiento y la continuidad de la red.

Datos de contacto:

European Judicial Network.
Johan de Wittlaan 9
2517 JR The Hague
Netherlands
E-mail: info@eurojust.europa.eu
Telephone: +31 70 412 5000
Fax: +31 70 412 5005

⁸⁹⁴ Cuando en los diferentes textos se refiere a la Decisión de la RJE, se está aludiendo a este documento normativo del año 2008.

SITCEN (CENTRO CONJUNTO DE SITUACIÓN DE LA UNIÓN EUROPEA)

SITCEN surgió como una red abierta de inteligencia para el intercambio de información entre EUROPOL y los EEMM. Con sede en Bruselas, dependía inicialmente de la Secretaria General Unión Europea.

Al momento de su creación, en el año 2002, el centro contaba con un numero restringido de expertos en servicios de inteligencia exterior de la UE

En el año 2004 se presentó al Consejo de la Unión Europea un documento cuyo contenido planteaba la mejora de los servicios de inteligencia. Se presentaron propuestas para mejorar la red a fin de que pueda analizar no solo de la situación exterior (amenazas externas de la UE), sino también la interior (seguridad interna de la UE y terrorismo). Este centro mejorado, caracterizado por la idea modélica de una CIA europea, se implementó en el año 2005. Posteriormente tuvieron lugar diferentes adaptaciones y mejoras que permitieron una gran evolución del centro de inteligencia.

En el año 2012, SITCEN pasó a llamarse Centro de Análisis de Inteligencia de la Unión Europea (EU INTCEN), y finalmente en el año 2015 adoptó su nombre actual: Centro de Inteligencia y Situación de la UE (EU INTCEN).

Centro reemplazado por EU INTCEN en el año 2012. Ver: EU INTCEN (CENTRO DE INTELIGENCIA Y SITUACIÓN DE LA UE).

SEAE (SERVICIO EUROPEO DE ACCION EXTERIOR)

El Servicio Europeo de Acción Exterior (SEAE) es el servicio diplomático de la UE. El SEAE fue creado en el año 2007, en el marco del Tratado de Lisboa. Sin embargo, recién en el año 2011 se estableció de manera formal. Como servicio diplomático de la UE, el SEAE asiste al Alto Representante de la UE para Asuntos Exteriores y Política de Seguridad y Vicepresidente de la Comisión Europea (AR/VP) en el desarrollo de la Política Exterior y de Seguridad de la UE.

El SEAE trabaja de manera conjunta con los Ministerios de Asuntos Exteriores y de Defensa de los EEMM, y con otras instituciones europeas como la Comisión Europea, el Consejo de la Unión Europea y el Parlamento. Posee una relación estrecha con la ONU y con otras Organizaciones Internacionales. La sede del SEAE se encuentra en Bruselas, cuenta con una red de delegaciones diplomáticas en Estados europeos y terceros Estados.

Datos de contacto:

European External Action Service.
EEAS Building
9A Rond Point Schuman
1046 Bruxelles/Brussel
Belgique/België
Telephone: +32 2 584 11 11
Fax: +32 2 584 11 11

ANEXOS

ANEXO N.º 01: ORIGEN Y EVOLUCIÓN DE LA UNIÓN EUROPEA

2022



ORIGEN Y EVOLUCIÓN DE LA UNIÓN EUROPEA



ORIGEN Y EVOLUCIÓN DE LA UNIÓN EUROPEA 2022



Este capítulo ha sido elaborado por: Centro de Documentación Europea y Europe Direct

COMUNIDAD DE MADRID

2022





El origen de la actual Unión Europea se sitúa el **9 de mayo de 1950**. Ese día, Robert Schumann (Ministro francés de Asuntos Exteriores) hizo pública una Declaración dirigida a Alemania en la que propuso poner el conjunto de la producción franco-alemana de carbón y acero bajo una alta autoridad común, creando al mismo tiempo una organización abierta a la participación de los demás países de Europa. Con esta Declaración, Francia proponía públicamente a Alemania dejar atrás sus tradicionales diferencias, con el fin de establecer unas bases comunes de desarrollo económico.

Nació así la **Comunidad Europea del Carbón y del Acero (CECA)**, cuyo tratado constitutivo, el **Tratado de París**, fue firmado el **18 de abril de 1951** y entró en vigor el 25 de julio de 1952 para sus seis países firmantes: Francia, Alemania, Italia, Bélgica, Países Bajos y Luxemburgo (el Tratado fue firmado para un periodo de 50 años, por lo que expiró en julio de 2002).

En su voluntad de seguir adelante en la construcción europea, los seis países signatarios de la CECA firmaron seis años más tarde (el **25 de marzo de 1957**) los **Tratados de Roma** que instituyen la Comunidad Económica Europea (CEE) y la **Comunidad Europea de la Energía Atómica (CEEa)**. Estos tratados entraron en vigor el 1 de enero de 1958 por un período ilimitado de tiempo.

La CECA y la CEEa fijaron unos objetivos económicos específicos, y en unos ámbitos económicos determinados (el carbón y el acero, y la energía atómica, respectivamente) pero la CEE estableció unos objetivos más ambiciosos y más generales: “sentar las bases de una unión cada vez más estrecha entre los pueblos europeos”, “asegurar (...) el progreso económico y social de los respectivos países”, y eliminar las barreras que dividían Europa para consolidar “la defensa de la paz y la libertad”. Para ello, el Tratado de la CEE proponía establecer un mercado común que garantizara la libre circulación de mercancías, servicios, personas y capitales, y aproximar progresivamente las políticas económicas de los Estados miembros (en particular las políticas agrícolas, de transporte y comercio, y las reglas de la competencia y de la transparencia de precios).

Para conseguir los objetivos marcados, los Tratados de París y de Roma establecieron las bases de una arquitectura comunitaria. En un principio lo hicieron de forma parcialmente independiente (sólo la Asamblea Parlamentaria y el Tribunal de Justicia eran comunes a las tres Comunidades), pero el **8 de abril de 1965** se firmó en Bruselas el **Tratado de fusión de los Ejecutivos** (entrando en vigor el 1 de enero de 1967), por el que se constituía un Consejo único y una Comisión única para las tres Comunidades. De esta forma quedaba establecido el siguiente marco institucional único:

- La **Comisión**, encargada de velar por la correcta aplicación de los Tratados.
- El **Consejo de Ministros**, sobre el que descansa el poder decisorio.
- El **Parlamento Europeo**, representante de todos los ciudadanos.
- El **Tribunal de Justicia**, cuya misión es la de asegurar el control jurisdiccional.

A estas instituciones se les unió, en 1975, el **Tribunal de Cuentas** (creado por el Tratado de 22 de julio de 1975), con la misión de efectuar un control externo del presupuesto comunitario, examinando para ello el equilibrio entre ingresos y gastos.

Los positivos efectos que la creación de las Comunidades Europeas tuvo para la economía de los Estados miembros, llevaron a otros países europeos a solicitar la adhesión. Así, las Comunidades Europeas se fueron ampliando, sucesivamente, al **Reino Unido, Irlanda y Dinamarca** (en **1973**), a **Grecia** (en **1981**),



a **España y Portugal** (en **1986**), a **Austria, Suecia y Finlandia** (en **1995**), a **Polonia, Hungría, República Checa, Eslovaquia, Eslovenia, Estonia, Letonia, Lituania, Malta y Chipre** (en **2004**), a **Rumanía y Bulgaria** (en **2007**) y por último a **Croacia** (en **2013**). La Unión Europea actual también identifica un grupo de países candidatos, aún sin fecha prevista de adhesión, que son: Antigua República Yugoslava de Macedonia, Islandia, Montenegro, Serbia y Turquía. Además incluye como candidatos potenciales a Bosnia y Herzegovina, Kosovo y Albania.

Paralelamente a las ampliaciones de las Comunidades Europeas, se producían avances en materia política, económica y social. Todo ello ha exigido profundas reformas en los sistemas jurídicos e institucionales, con el fin de adaptar las originarias estructuras a las necesidades que iban surgiendo.

En lo que respecta a los Tratados, en tanto que creadores de las Comunidades Europeas, ha sido necesario reformarlos en varias ocasiones, con objeto de incorporar a los textos constitutivos las sucesivas modificaciones que se iban aprobando. Las modificaciones más importantes han sido las siguientes:

- El 22 de abril de 1970 se firma en Luxemburgo el ***Tratado por el que se modifican determinadas disposiciones presupuestarias de los Tratados Constitutivos de las Comunidades Europeas y del Tratado por el que se constituye un Consejo único y una Comisión única de las Comunidades Europeas***. Entonces, las Comunidades introducirán las reformas necesarias para disponer, a partir de 1975, de un presupuesto **financiado íntegramente con recursos propios**, y que cubra la totalidad de sus gastos.
- La Decisión del Consejo de 20 de septiembre de 1976 esta acompañada del Acta relativa a la elección de los representantes en Asamblea por sufragio universal directo. Desde este momento, los representantes que componen la Asamblea parlamentaria serán elegidos por **sufragio universal directo** y por un periodo de cinco años.
- En 1986, los 12 Estados miembros de las Comunidades Europeas firman el **Acta Única Europea**, primera gran reforma de los Tratados. El Acta Única Europea introdujo modificaciones que afectaron profundamente a la estructura comunitaria:
 - Incrementó el papel e influencia del Parlamento Europeo frente al resto de Instituciones.
 - Aumentó la institucionalización de las reuniones de Jefes de Estado o de Gobierno (denominadas Consejos Europeos o, más popularmente, Cumbres).
 - Realizó nuevas transferencias de competencias estatales a favor de las Comunidades, a fin de facilitar la consecución de un verdadero mercado único interior (un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estuvieran garantizadas).
 - Sentó las bases para la creación, dos años más tarde, del Tribunal de Primera Instancia (agregado al Tribunal de Justicia que ya existía).
 - Introdujo la regulación de la cooperación política europea en materia de política exterior.
- Seis años más tarde, en 1992 se produjo la más importante reforma de los Tratados fundacionales con la firma en Maastricht del **Tratado de la Unión Europea**. Este Tratado modificó ampliamente los Tratados constitutivos de las Comunidades Europeas, e introdujo cuatro nuevos objetivos:



- Asegurar el progreso económico y social equilibrado y sostenible, para lo que se estableció una Unión Económica y Monetaria.
- Reforzar la protección de los derechos e intereses de los nacionales de cada Estado miembro, mediante la creación de una “ciudadanía de la Unión”. Esta nueva ciudadanía no se presenta como sustituta, sino como complementaria de la nacionalidad.
- Realizar una política exterior y de seguridad común, y una política exterior de seguridad y defensa.
- Aumentar la cooperación policial y judicial, con el fin de lograr la plena y segura libertad de circulación de las personas dentro del territorio de la Unión.

La **Comunidad Económica Europea (CEE)** perdió su adjetivo de “económica”, pasando a denominarse simplemente Comunidad Europea (CE), con el fin de adecuar su denominación a su nuevo papel en el proceso de integración europea. Pero la novedad más importante del Tratado, fue la creación de una “Unión Europea” entre los Estados miembros. Esta Unión fue formada sobre las tres Comunidades Europeas, a las que se les añadieron dos nuevos ámbitos: las cooperaciones en Política Exterior y de Seguridad común, y en los Asuntos de Justicia e Interior. Estas cooperaciones tienen carácter intergubernamental, lo cual quiere decir que siguen siendo plenamente de soberanía nacional no utilizan el método de la integración o transferencia de competencias, propio de las Comunidades Europeas, sino el de la simple cooperación entre gobiernos.

La estructura de la Unión Europea, de acuerdo con el Tratado, quedó integrada por tres pilares:

- **Primer Pilar:** Constituido por las tres Comunidades Europeas (CECA, CE y CEEA). Además, el Tratado de la Unión fortaleció las instituciones comunitarias: el Parlamento Europeo vio reforzados sus poderes al introducirse el procedimiento de codecisión (en el que el Parlamento y el Consejo se convierten en colegisladores) y se fortalecieron sus poderes de control político y financiero sobre la Comisión Europea. Por su parte, la Comisión incrementó sus competencias en los ámbitos de salud pública, cultura, protección de los consumidores, educación, industria, redes transeuropeas y cooperación al desarrollo. Y el Consejo, aumentó su capacidad de decisión al aumentar el número de supuestos en que las decisiones se toman por mayoría cualificada.

Por otro lado, se reforzó la política de cohesión económica y social al crearse como instrumento el Fondo de Cohesión, del que se benefician los Estados miembros con menor renta comunitaria, y que se destina a financiar principalmente las infraestructuras de transporte y las acciones de medio ambiente.

Se crearon nuevos derechos para los ciudadanos, y se aumentó su protección con la creación del Defensor del Pueblo Europeo.

- **Segundo Pilar:** Constituido por la Política Exterior y de Seguridad Común (popularmente denominada PESC). Esta política se enmarca en el ámbito de una cooperación intergubernamental, y tiene como objetivos el fortalecimiento de la seguridad de la Unión, el mantenimiento de la paz y seguridad internacional, el fomento de la cooperación internacional, el desarrollo y consolidación de la democracia y del Estado de Derecho, así como el respeto de los Derechos Humanos y las Libertades Fundamentales.

- **Tercer Pilar:** Basado en una cooperación intergubernamental en los ámbitos de la Justicia y Asuntos de Interior. Su objetivo es ofrecer a los ciudadanos un nivel elevado de protección mediante el control de las fronteras exteriores, la política de asilo y de inmigración, la cooperación judicial y la lucha contra el fraude.



- En 1997 se firmó un nuevo **Tratado** en la ciudad de **Ámsterdam**. El Tratado incluyó algunas reformas positivas, especialmente en lo que respecta al Parlamento Europeo (al que reforzó, aumentando sus competencias), pero en general, fue insuficiente e ineficaz en sus modificaciones. Faltaron los acuerdos en temas de gran importancia (como por ejemplo en lo relativo a la futura composición de la Comisión, la ponderación de votos en el Consejo, o a la fusión y reestructuración de los Tratados en un único texto jurídico), y las novedades que incorporaba resultaron, en ocasiones, directamente inviables (como en el caso de las “cooperaciones reforzadas”, difíciles de aplicar ante la cantidad de requisitos que se exigían). El propio Tratado de Ámsterdam, consciente de sus limitaciones, se encargaba de anunciar nuevas reformas antes de la siguiente ampliación de la Unión Europea.

- El Consejo Europeo de Colonia del 3 y 4 de junio de 1999 decidió iniciar la redacción de una **Carta de Derechos Fundamentales** para reunir todos aquellos derechos fundamentales en vigor en la Unión en un único texto y darles así mayor relevancia. Esta Carta se basa en los Tratados comunitarios, los convenios internacionales (incluidos el Convenio Europeo de Derechos Humanos de 1950 y la Carta Social Europea de 1989), las tradiciones constitucionales comunes de los Estados miembros y distintas declaraciones del Parlamento Europeo.

La elaboración de la Carta se confió a una Convención, compuesta por 62 representantes de los Jefes de Estado y de Gobierno de los Estados miembros, del Presidente de la Comisión Europea, del Parlamento Europeo y de los parlamentos nacionales. También asistieron cuatro observadores del Tribunal de Justicia de la Unión Europea, del Consejo de Europa y del Tribunal Europeo de Derechos Humanos. El resultado de los trabajos fue presentado en el Consejo Europeo de Biarritz (13 y 14 de octubre del 2000): una Carta de Derechos Fundamentales que define en 54 artículos los derechos fundamentales referentes a la dignidad, libertad, igualdad, solidaridad, ciudadanía y justicia.

- El 26 de febrero de 2001 se adoptó el **Tratado de Niza**. El Tratado entró en vigor el 1 de febrero de 2003 tras la ratificación por los entonces quince Estados miembros de la Unión Europea. Su principal objetivo era preparar a la Unión Europea para la inminente ampliación, revisando los Tratados en cuatro cuestiones principales: tamaño y composición de la Comisión, ponderación de votos en el Consejo, ampliación de la votación por mayoría cualificada y las cooperaciones reforzadas.

El Tratado de Niza no introduce cambios importantes en el equilibrio institucional, pero sí supone un ajuste en lo que respecta al funcionamiento y a la composición de las instituciones (especialmente en cuanto al reparto del número de diputados y de votos en cada Institución) y muy especialmente respecto al funcionamiento de las cooperaciones reforzadas (flexibilizó el sistema al exigir condiciones menos estrictas, suprimir el derecho de veto y ampliar los ámbitos de aplicación). También modificó los procedimientos de decisión, al ampliar la votación por mayoría cualificada a una treintena de nuevas disposiciones.

El Tratado de Niza pretendió establecer las normas de funcionamiento para una Unión Europea ampliada. Pero lo cierto es que en el momento de la redacción del Tratado se desconocía el momento y el orden en el que se llevaría a cabo la adhesión de los países candidatos de la Unión. Por ello, el Tratado se limitó a establecer los principios y métodos que se debían utilizar para:

- Establecer la nueva composición de la Comisión.
- Definir la mayoría cualificada del Consejo.



- Fijar el número definitivo de escaños de los nuevos Estados miembros en el Parlamento y el número de votos que se les atribuirían en el Consejo.
- Determinar el umbral de la mayoría cualificada a aplicar en el futuro.

Todas estas cuestiones han sido jurídicamente establecidas en el **Tratado de Adhesión** de los diez nuevos Estados miembros, suscrito en **Atenas el 16 de abril de 2003**, que modifica los Tratados de la Unión Europea y de la Comunidad Europea.

- Como resultado final de la Unión económica y monetaria, el 1 de enero de 2002 se introdujo en casi todos los países que entonces formaban la Unión Europea, una moneda única: **el euro**. El 28 de febrero de 2002, finalizó la fase transitoria de la doble circulación de las antiguas monedas y del euro, y este último pasó a ser, desde entonces, la moneda única para más de 300 millones de europeos.
- Las tradicionales revisiones de los Tratados Europeos habían sido preparadas por una Conferencia Intergubernamental (CIG) que reunía a representantes de los Gobiernos de los Estados miembros y unificaba las distintas soluciones presentadas. Sin embargo, a la vista de los últimos resultados, el sistema se reveló claramente insuficiente, pues numerosas cuestiones institucionales fundamentales en vísperas de la ampliación, habían quedado sin una respuesta eficaz. Por ello, después del Tratado de Niza se impuso la necesidad de intentar una reforma institucional que fuera más allá de la simple adaptación de las instituciones con vistas a la ampliación. Y, al mismo tiempo, se planteó la necesidad de instaurar un debate más amplio y profundo sobre el futuro de la Unión Europea.

En su reunión de Laeken de diciembre de 2001, el Consejo Europeo presentó la convocatoria de una Convención que preparara la siguiente CIG de una forma amplia, pública, e involucrando a las principales partes interesadas: representantes de los gobiernos de los Estados miembros y los países candidatos, representantes de los parlamentos nacionales, representantes del Parlamento Europeo y de la Comisión Europea, y observadores del Comité de las Regiones, el Comité Económico y Social Europeo y los interlocutores sociales europeos.

La Convención comenzó sus trabajos a principios de 2002, y los concluyó el 18 de julio de 2003 con la entrega de la Presidencia italiana del **Proyecto final de Tratado por el que se instituye una Constitución para Europa**, por parte de su Presidente, Sr. D. Valéry Giscard d'Estaing.

Tras un extenso debate sobre el texto constitucional, en el Consejo Europeo celebrado los días 17 y 18 de junio de 2004 en Bruselas, se acordó el texto definitivo dando paso a la fase de ratificación. Para su entrada en vigor el texto debía ser ratificado por todos los Estados miembros, con arreglo a sus respectivas normas constitucionales, mediante ratificación parlamentaria o referéndum del pueblo. En el texto presentado se preveía la duración máxima del proceso de ratificación en dos años, esto es, el 1 de noviembre de 2006 como fecha límite para dicha ratificación. Debido a las dificultades de ratificación que se produjeron en determinados Estados miembros (principalmente Francia y Países Bajos que rechazaron el Proyecto) y ante la posibilidad de una crisis institucional, se inició un periodo de reflexión que dio lugar a la transformación del primer proyecto de Constitución en un Tratado de Reforma de la Unión Europea.

- El **13 de diciembre de 2007** se firma el **Tratado de Lisboa**, ofreciendo una solución al debate constitucional e institucional, y el mismo entra en vigor el 1 de diciembre de 2009.



La Unión Europea define la finalidad del Tratado principalmente sobre los siguientes puntos:

- Aumento de las competencias del Parlamento Europeo.
- Cambio de los procedimientos de voto en el Consejo.
- Iniciativa ciudadana.
- Carácter permanente del puesto de Presidente del Consejo Europeo.
- Nuevo puesto de Alto Representante para Asuntos Exteriores.
- Renovación del servicio diplomático de la Unión Europea.

En síntesis, quedan definidas en este Tratado las atribuciones de competencia, tanto a la Unión como a los Estados miembros, así como aquellas competencias que serán compartidas.

Nos encontramos ante un Tratado que dota a la Unión de unas instituciones más modernas y adaptadas al nuevo panorama mundial, así como perfecciona los métodos de trabajo para poder afrontar problemas globales (cambio climático, globalización, evolución demográfica, seguridad y energía). Aparece una Unión Europea más democrática y más preparada para defender día a día los intereses de los ciudadanos europeos.

• Otra cuestión es la proclamación el **7 de diciembre de 2000 en Niza**, de la **Carta de los Derechos Fundamentales de la Unión Europea**, que es un documento que contiene una lista articulada de derechos humanos proclamada por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea. La carta no forma parte del Tratado de Lisboa (estaba previsto que formara parte de la Constitución Europea, pero al no aprobarse, se modificó la previsión), pero por la remisión en el artículo 6 del Tratado de la Unión Europea tras la reforma de Lisboa se hace vinculante para todos los estados, con la excepción de Polonia y Reino Unido. Por primera vez, se reunieron en un único documento todos los derechos que hasta ahora se repartían en distintos instrumentos legislativos como las legislaciones nacionales y los convenios internacionales del Consejo de Europa, de las Naciones Unidas y de la Organización Internacional del Trabajo. Por ello, contribuye a desarrollar el concepto de ciudadanía de la Unión Europea, así como a crear un espacio de libertad, seguridad y justicia. También refuerza la seguridad jurídica por lo que se refiere a la protección de los derechos fundamentales, que desde 1969 se garantizaba mediante la jurisprudencia del Tribunal de Justicia de la Unión Europea y con la actual redacción del Artículo 6 del Tratado de la Unión Europea.

• **Desde 2010**, la Unión Europea está afrontando nuevos problemas y retos. La crisis económica mundial golpeó de lleno Europa. La UE ha estado ayudando a varios países a hacer frente a sus dificultades y estableció la “unión bancaria” para crear un sector bancario más seguro y fiable. **En 2011**, el lanzamiento de los dos primeros satélites Galileo supone un avance hacia el sistema europeo de navegación por satélite. Esto contribuirá a mejorar el transporte, los servicios de emergencia, las transacciones bancarias y el suministro de electricidad. **En 2012**, la Iniciativa Ciudadana Europea es operativa y da a los ciudadanos la posibilidad de proponer a la Comisión Europea la creación de disposiciones legislativas. Además se otorga a la UE el Premio Nobel de la Paz, por “haber contribuido al desarrollo de la paz, la reconciliación, la democracia y los derechos humanos en Europa durante más de seis décadas”. **En 2013** Croacia se convierte



en el 28º miembro de la UE. **En 2014** se celebran las elecciones europeas y los euroescépticos ganan escaños en el Parlamento Europeo. Se establece una nueva política de seguridad a raíz de la anexión de Crimea a Rusia. Aumenta el extremismo religioso en Oriente Próximo y en diversos países y regiones de todo el mundo, dando lugar a revueltas y guerras que llevan a muchas personas a huir de sus hogares y buscar refugio en Europa. La UE no solo se enfrenta al dilema de cómo atenderlos, sino que también es objetivo de varios ataques terroristas. En diciembre de **2015**, como el cambio climático sigue teniendo un lugar destacado en la agenda de la UE, los dirigentes acuerdan reducir las emisiones nocivas en la Conferencia sobre el Cambio Climático de París, donde se ponen de acuerdo 195 países para limitar el aumento de la temperatura mundial a menos de 2 °C.

- Una fecha clave reciente es el **23 de junio de 2016**, cuando se celebró en Reino Unido un Referéndum sobre la permanencia o no del país en la Unión Europea, fenómeno que se ha denominado **“Brexit”**. Por primera vez en la historia de las comunidades europeas, un país solicitó su salida acogiéndose al artículo 50 del Tratado de Lisboa. El **29 de marzo de 2017**, siendo Jefa de Gobierno Theresa May, la Unión Europea recibió una carta que activó el proceso de salida del Reino Unido. La desconexión deberá hacerse efectiva, según los planes previstos, el 29 de marzo de 2019. El país deberá negociar un nuevo acuerdo con la UE y transponer el derecho comunitario a su legislación.

- En abril de 2017, la Comisión Europea publicó un documento de reflexión sobre la dimensión social de Europa basado en el Libro Blanco sobre el futuro de Europa. Empezó un proceso de reflexión con los ciudadanos, los interlocutores sociales, las instituciones europeas y los gobiernos en el que se trata de determinar qué respuesta debe darse a los desafíos a que se enfrentarán los ciudadanos y las sociedades en los próximos años y de aclarar la contribución de la UE a dicha respuesta.

- En Junio, Estonia asumió la Presidencia del Consejo de la Unión Europea. Sus cuatro prioridades fueron: una economía europea innovadora y abierta, una Europa segura y protegida, la Europa digital y la libre circulación de los datos, y una Europa integradora y sostenible.

- También se celebraron los 30 años del programa Erasmus de intercambios en el extranjero, del que se han beneficiado hasta ahora 9 millones de personas en toda Europa.

- Además se acabaron los costes de itinerancia por la utilización de teléfonos móviles en el extranjero. A partir de esta fecha las personas que viajen por la UE pueden realizar llamadas, enviar mensajes de texto y conectarse a internet al mismo precio que en su país de origen.

- En Septiembre, el Acuerdo Económico y Comercial Global (AECG) entre la UE y Canadá entró en vigor de manera provisional: estará plena y definitivamente vigente cuando todos los Estados miembros de la UE lo hayan ratificado.

- En diciembre, la Comisión Europea lanzó el Año Europeo del Patrimonio Cultural 2018, cuyo objetivo es dar a conocer la riqueza del patrimonio cultural europeo y su papel en la construcción de un sentimiento de identidad compartida.

- Además, la UE y Japón celebraron un histórico acuerdo de libre comercio. El Acuerdo de Asociación Económica abre el mercado japonés a las principales



exportaciones agrícolas de la UE y aumenta las posibilidades de exportación para Europa en toda una serie de sectores.

- También, el Consejo estableció un marco permanente para la cooperación en materia de defensa. Los 25 Estados miembros participantes en la Cooperación Estructurada Permanente (PESCO) presentaron sus planes para una primera tanda de 17 proyectos colaborativos.
- Para terminar el año, la Comisión tomó medidas sin precedentes contra Polonia al concluir que hay claro riesgo de violación grave del Estado de Derecho debido a una serie de reformas que amenazan a la independencia judicial en este país.
- En Enero de 2018, Bulgaria asumió por primera vez la Presidencia semestral rotatoria del Consejo de la Unión Europea. El programa fijó prioridades en cuatro ámbitos clave: el futuro de Europa y los jóvenes, la perspectiva europea y la conectividad en los Balcanes Occidentales, seguridad y estabilidad y economía digital.
- Entraron en vigor nuevas normas para evitar la evasión fiscal y el blanqueo de capitales. Las nuevas disposiciones obligan a los Estados miembros a dar acceso a las autoridades tributarias a los datos recogidos con arreglo a la legislación contra el blanqueo de capitales.
- La Comisión Europea presentó la primera estrategia sobre los plásticos para toda Europa, que forma parte de la transición hacia una economía más circular. Se puso en marcha en Bruselas el Observatorio de la Pobreza Energética, que forma parte de los esfuerzos de la Comisión por combatir la pobreza energética en los países miembros. Se engloba en la aplicación del pilar europeo de derechos sociales y es una de las medidas que intentan apoyar una transición justa y socialmente equitativa hacia una energía limpia.
- Además, la Comisión Europea adoptó una estrategia para la adhesión de seis países socios de los Balcanes Occidentales a la Unión Europea. Serbia y Montenegro son los primeros candidatos que podrían estar listos para la adhesión en 2025.
- La Comisión Europea publica el proyecto de acuerdo de retirada entre la Unión Europea y el Reino Unido.
- En marzo en consonancia con el compromiso del presidente Juncker de alcanzar una auténtica Unión de Defensa a más tardar en 2025, la Comisión y la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad presentan un plan de acción para mejorar la movilidad militar dentro y fuera de la Unión Europea.
- El sistema automático de llamadas de emergencia, eCall se hace obligatorio en toda la UE para los vehículos nuevos, con el objetivo de salvar más vidas en las carreteras. El sistema marca automáticamente el número 112, el número único de emergencia europeo, cuando tiene lugar un accidente grave.
- En abril, entran en vigor nuevas normas de la UE que permiten que las personas que compran o se abonan a servicios de contenidos online para acceder a películas o transmisiones deportivas, música, libros electrónicos o juegos puedan acceder también a ellos cuando viajen a otro país de la UE.



- La Unión Europea y México alcanzan un nuevo acuerdo sobre comercio. Este acuerdo, que formará parte de un acuerdo global modernizado más amplio entre la UE y México, profundizará y ampliará el ámbito de aplicación del actual acuerdo comercial firmado en 1997.
- En mayo, para crear un entorno más seguro y favorable al comercio entre la UE y Nueva Zelanda, entra en vigor un nuevo acuerdo aduanero. El acuerdo hará posible la colaboración de las partes a fin de prevenir, investigar y combatir las infracciones de la normativa aduanera.
- El 25 de mayo de 2018 entró en vigor el Reglamento general de protección de datos de la Unión Europea.
- En junio, los ministros de la UE adoptan formalmente la revisión de la legislación de la UE en materia de seguridad aérea. Se incluyen las primeras normas de la UE para aeronaves civiles no tripuladas (drones) de todos los tamaños, por las que se establecen principios fundamentales en materia de seguridad, protección, privacidad, protección de datos y protección del medio ambiente.
- En julio la UE celebró el 50 aniversario de la unión aduanera con diversos actos ya que se ha convertido en una de las piedras angulares del mercado único, manteniendo la seguridad de las fronteras de la UE y protegiendo a los ciudadanos frente a mercancías prohibidas y peligrosas como las armas y las drogas.
- Entraron en vigor nuevas normas de la UE que garantizan una mayor protección para los usuarios de servicios turísticos. Además de reforzar los derechos de los consumidores que reservan paquetes turísticos tradicionales, las nuevas normas también protegen a los usuarios de otras modalidades de viaje combinado.
- También entraron en vigor normas de la UE reforzadas para impedir el blanqueo de capitales y conjurar los riesgos de financiación del terrorismo así como las nuevas normas de rendimiento energético con enorme potencial para incrementar la eficiencia energética del sector de la construcción de la UE, principal consumidor europeo de energía.
- La UE y Japón firman un histórico acuerdo comercial, el mayor jamás negociado por la UE, y un acuerdo de asociación estratégica para intensificar la cooperación en una serie de ámbitos. La UE y Japón también finalizan las negociaciones para reconocer mutuamente como “equivalentes” sus sistemas respectivos de protección de datos.
- En septiembre de 2018 entraron en vigor en la UE nuevas normas sobre la utilización transfronteriza de medios de identificación electrónica, como tarjetas de identidad, permisos de conducción y tarjetas bancarias. Esto permitirá a los ciudadanos y las empresas de la UE acceder a los servicios en línea aunque sean de otro Estado miembro.
- En diciembre de 2018 se adoptaron nuevas normas que permiten a los consumidores europeos comprar online en la UE sin sufrir bloqueos ni desvíos. Esta legislación forma parte de una serie de nuevas normas sobre comercio electrónico cuya finalidad es impulsar las ventas transfronterizas online en la UE, en beneficio tanto de los consumidores como de los vendedores online.



- También en vigor en toda la UE normas más estrictas que penalizan el blanqueo de capitales. Las nuevas normas garantizarán que los terroristas y los delincuentes peligrosos se enfrenten a graves sanciones por blanqueo de capitales dondequiera que estén en la UE, con un mínimo de cuatro años de prisión. Los Estados miembros disponen de 24 meses para incorporar las nuevas normas al Derecho nacional.
- Para finalizar el año, entraron en vigor tres actos legislativos esenciales para facilitar la transición a las energías limpias en Europa. El nuevo marco político fija dos nuevos objetivos para la UE para 2030: un objetivo vinculante de al menos un 32% de energía renovable y un objetivo de eficiencia energética de al menos el 32,5%, con una posible revisión al alza en 2023. Asimismo, introduce los primeros planes nacionales en materia de clima y energía, que describen la manera en que los Estados miembros alcanzarán sus objetivos respectivos.
- Y por último, las nuevas normas para reforzar el Sistema de Información de Schengen, el sistema de intercambio de información más utilizado para la gestión de las fronteras y la seguridad en Europa.
- En enero de 2019, el euro cumplió 20 años. En la actualidad, es utilizado por más de 340 millones de ciudadanos en 19 países de la UE y es la segunda moneda más importante del mundo.
- Se empezaron a aplicar nuevas normas:
 - para luchar contra las principales formas de elusión fiscal practicada por las grandes empresas multinacionales.
 - sobre los fondos de pensiones de empleo, que fomentan y facilitan el acceso a las pensiones de jubilación, mejoran y modernizan la manera en que los fondos de pensiones se rigen y aumentan la claridad de la información facilitada a los partícipes y beneficiarios de fondos de pensiones.
 - se pone en marcha una nueva iniciativa sanitaria de la UE que permite a los pacientes utilizar las recetas electrónicas en otro país de la UE.
 - comienzan a aplicarse en 18 Estados miembros nuevas normas que aclaran los derechos de propiedad de las parejas internacionales casadas o en una unión registrada. Los nuevos Reglamentos establecen normas claras para los casos de divorcio o fallecimiento, poniendo con ello fin al desarrollo de procedimientos paralelos y acaso contradictorios en varios Estados miembros, en relación, por ejemplo, con el patrimonio o las cuentas bancarias.
- En febrero entró en vigor el acuerdo comercial entre la UE y Japón, conformando la mayor zona de comercio abierto del mundo.
- Empiezan a aplicarse en toda la UE nuevas normas para:
 - lograr que la detección de medicamentos falsos sea más fácil y eficaz.
 - reducir los costes y trámites de los ciudadanos que viven o trabajan en otro Estado miembro.
 - proteger al 100% de los agricultores europeos, así como a los proveedores pequeños y medianos, de las prácticas comerciales desleales en la cadena de suministro alimentario.



- Entra en funcionamiento rescEU, el nuevo sistema para reforzar la respuesta colectiva de la UE ante las catástrofes naturales.
- Entra en vigor el primer marco de la Unión para controlar las inversiones extranjeras directas en la UE.
- Los líderes de los Veintisiete acuerdan aplazar el Brexit. Esta decisión se toma de acuerdo con el Reino Unido. La duración de la prórroga se limitará a lo necesario, sin rebasar en ningún caso la fecha del 31 de octubre de 2019.
- Sin embargo, el 28 de octubre, el Consejo Europeo adoptó una Decisión por la que se prorroga el plazo previsto en el artículo 50, apartado 3 del Tratado de la Unión Europea, en el contexto de la intención del Reino Unido de retirarse de la U.E. La prórroga durará hasta el 31 de enero de 2020 para dejar más tiempo para la ratificación del Acuerdo de Retirada. La retirada puede producirse antes, el 1 de diciembre de 2019 o el 1 de enero de 2020, en caso de que ambas partes ratifiquen el Acuerdo de Retirada.
- En noviembre de 2019, El Parlamento Europeo aprueba el nuevo colegio de 26 comisarios, presentado por la presidenta electa Ursula von der Leyen, por 461 votos a favor, 157 en contra y 89 abstenciones.
- En vísperas de la Conferencia de las Naciones Unidas sobre el Cambio Climático en Madrid, el Parlamento Europeo aprueba una Resolución que declara la emergencia climática y medioambiental en Europa y en todo el mundo.
- En diciembre de 2019, la UE celebra el 10º aniversario de la Carta de los Derechos Fundamentales de la UE que consagra una serie de derechos y libertades individuales. La Carta pasó a ser jurídicamente vinculante al entrar en vigor el Tratado de Lisboa, el 1 de diciembre de 2009.
- La Comisión Von der Leyen presenta su política prioritaria, el Pacto Verde Europeo, que describe cómo convertir Europa en el primer continente climáticamente neutro de aquí a 2050.
- En Enero de 2020, Croacia asume por primera vez la Presidencia semestral rotatoria del Consejo de la Unión Europea.
- El Parlamento Europeo aprueba el acuerdo para la salida del Reino Unido de la UE por 621 votos a favor, 49 en contra y 13 abstenciones. El Consejo adopta, en nombre de la UE, la decisión sobre la celebración del Acuerdo de Retirada del Reino Unido de la Unión Europea. Previamente, el 29 de enero el Parlamento Europeo había aprobado dicho acuerdo, firmado por la UE y el Reino Unido el 24 de enero.
- La UE anuncia que destinará 10 millones de euros a la investigación del nuevo brote de coronavirus. La enfermedad se detectó en China a finales de 2019 y los primeros casos europeos se notificaron a finales de enero de 2020. La Comisión también colabora estrechamente con la Organización Mundial de la Salud y otros agentes internacionales para garantizar una respuesta eficaz y coordinada al brote.
- En marzo de 2020, La Comisión crea un «equipo de respuesta al coronavirus» para coordinar la gestión del brote de COVID-19.



- La Comisión propone la primera Ley del Clima Europea para consagrar en la legislación el compromiso político de la UE de alcanzar la neutralidad climática para 2050.
- El Parlamento Europeo celebra una reunión extraordinaria para adoptar medidas especiales a fin de hacer frente a los efectos de la pandemia de COVID-19 en los Estados miembros de la UE. Los eurodiputados participan y votan a distancia por primera vez en la historia del Parlamento para respetar las estrictas precauciones sanitarias.
- La Comisión Europea presenta directrices prácticas para garantizar la libre circulación de los trabajadores críticos y orientaciones sobre la aplicación de la restricción temporal de los viajes no esenciales a la UE. La UE también sigue trabajando en todos los frentes para ayudar a los ciudadanos europeos en todo el mundo que se ven afectados por las restricciones de viaje debidas al brote de coronavirus.
- En abril de 2020, En respuesta a la crisis del coronavirus, y para ayudar rápidamente a los trabajadores y limitar el riesgo de desempleo, la Comisión propone la creación una nueva iniciativa denominada SURE (Instrumento Europeo de Apoyo Temporal para Mitigar los Riesgos de Desempleo en una Emergencia).
- La Comisión Europea pone en marcha la plataforma europea de datos sobre la COVID-19 que permite recopilar y compartir rápidamente los datos de investigación disponibles.
- En mayo de 2020, La Unión Europea aúna esfuerzos con socios internacionales para poner en marcha una conferencia de donantes, la Respuesta mundial a la crisis del coronavirus, que recauda 7.400 millones de euros para el desarrollo e implantación de medios de diagnóstico, tratamiento e inmunización contra el coronavirus. El acto, que marca el inicio de un «maratón mundial de donantes», responde a llamamiento conjunto a la acción formulado por la Organización Mundial de la Salud (OMS) y diversas organizaciones sanitarias internacionales.
- La Comisión Europea presenta una nueva estrategia sobre la biodiversidad y una estrategia «de la granja a la mesa». En consonancia con el Pacto Verde Europeo, estas estrategias proponen medidas y compromisos ambiciosos por parte de la UE para detener la pérdida de biodiversidad en Europa y en el mundo y transformar los sistemas alimentarios de la UE.
- La Comisión Europea presenta su propuesta de gran plan de recuperación para Europa que contribuirá a reparar los daños económicos y sociales provocados por la pandemia de coronavirus, así como a forjar un futuro mejor para la próxima generación. El plan propone un nuevo instrumento de recuperación dotado de 750.000 millones de euros, denominado Next Generation EU. El instrumento quedará integrado en un presupuesto reforzado de la UE a largo plazo para el periodo 2021-2027, que elevará a 1,85 billones de euros la capacidad financiera total para relanzar la economía.
- Entre el 17 y el 21 de julio de 2020, se celebró un Consejo Europeo especial debido la crisis producida por el COVID-19 en donde la UE se ha enfrentado a un reto de proporciones históricas. Se adoptaron medidas de emergencia para preservar la salud de los ciudadanos y prevenir un colapso de la economía.
- El Reino Unido deja de ser miembro de la Unión Europea tras 47 años de pertenencia, lo que marca un nuevo capítulo de la historia de la Unión. La entrada



en vigor del Acuerdo de Retirada señala el inicio de un periodo transitorio hasta el 31 de diciembre de 2020, como mínimo, durante el cual el Reino Unido mantendrá su participación en el mercado único y la Unión Aduanera. Aunque la legislación de la UE se seguirá aplicando hasta el final del periodo transitorio en el Reino Unido, este dejará de tomar parte en los procesos de toma de decisiones de la UE, al ser ya un país que no forma parte de la Unión.

- En agosto de 2020, Estados Unidos y la Unión Europea alcanzan un acuerdo, para reducir los aranceles sobre determinados productos, las primeras reducciones de derechos negociadas entre la UE y los EE. UU. en más de dos décadas.
- La Comisión firma el primer contrato para la compra de una posible vacuna contra la COVID-19 con la empresa farmacéutica AstraZeneca. Esto supone un paso importante en la aplicación de la estrategia de la UE para las vacunas.
- En septiembre de 2020, la presidenta de la Comisión Europea, Ursula von der Leyen, pronuncia su primer discurso sobre el estado de la Unión ante el Parlamento Europeo (Bruselas). La presidenta plantea su visión para que la UE salga fortalecida de la pandemia de coronavirus y sobre las prioridades para el año próximo. Además, anuncia el plan de reducir de aquí a 2030 las emisiones de gases invernadero de la UE en un mínimo del 55% con respecto a los niveles de 1990. También se propone como objetivo que esta sea la “década digital” de Europa así como medidas para intensificar la lucha contra el racismo y un nuevo enfoque en materia de migración.
- En octubre, los Estados miembros de la UE acuerdan invertir casi 1.000 millones de euros en proyectos europeos clave de infraestructuras energéticas a través del Instrumento de Interconexión para Europa.
- La Comisión Europea presenta una serie de nuevas medidas de política energética para ayudar a construir una Europa climáticamente neutra.
- Entran en vigor en toda la UE nuevos procedimientos armonizados para hacer más eficaces, seguros y competitivos los ferrocarriles europeos.
- En noviembre, la Comisión Europea da los primeros pasos hacia la construcción de una Unión Europea de la Salud con propuestas para fortalecer el marco de seguridad sanitaria de la UE y reforzar la preparación frente a las crisis y la capacidad de respuesta de las principales agencias de la UE.
- Además, presenta la primera estrategia de la UE para la igualdad de las mujeres lesbianas, los hombres gays y las personas bisexuales, trans, no binarias, intersexuales y queer (LGBTIQ).
- En diciembre, la Comisión autoriza la primera vacuna segura y eficaz contra la COVID-19.
- En febrero de 2021, el Consejo adoptó el Reglamento por el que se establece el Mecanismo de Recuperación y Resiliencia, que constituye el núcleo del plan de recuperación de la UE.
- En mayo, la Comisión desembolsa 14.100 millones de euros a 12 Estados miembros a través del instrumento SURE.



- En junio, se pone en marcha el Certificado COVID Digital de la UE y a partir del 1 de julio comienza a usarse.
- En julio, se pone fin a los productos de plástico de un solo uso gracias a la Directiva sobre plásticos de un solo uso.
- Además, la Comisión Europea adoptó una serie de propuestas para adaptar las políticas de la UE en materia de clima, energía, transporte y fiscalidad con el fin de reducir las emisiones netas de gases de efecto invernadero en al menos un 55 % de aquí a 2030, en comparación con los niveles de 1990.
- En 2022, comienza como el Año Europeo de la Juventud, que pone el foco sobre la importancia de la juventud europea para construir un futuro mejor: más ecológico, más inclusivo y digital.
- El 24 de febrero de 2022, Europa amaneció con la desgarradora noticia de la agresión militar de Rusia a Ucrania. No se trata de un ataque tan solo contra Ucrania, sino también contra los valores de la Unión Europea.

https://europa.eu/european-union/about-eu/history/2020-today/2020_es

ANEXO N.º 02: DOCUMENTO PÚBLICO DE FUNCIONAMIENTO INTERNO DE PERCI

PUBLIC
Document made partially accessible
to the public on:
03 NOV 2022

PERCI TCO Regulation

Terrorism Working Party

Brussels, 20 September 2022

EU Internet Referral Unit
European Counter Terrorism Centre

 **EUROPOL**

Europol Unclassified - Basic Protection Level

PERCI

Plateforme Européenne de Retraits de Contenus Illégaux sur Internet

A single system to connect all EU MS and HSP for the facilitation of referrals and removal orders

TCO Recital 39 & article 14-4 MSs and HSPs encouraged to use dedicated tools, including those developed by Europol, to avoid duplication of effort and facilitate swift exchange between CAs and HSPs

BENEFITS FOR THE EU MS

Effectiveness

- Avoid the development of 27 national systems
- Save costs and time

Interoperability

- EU-wide cooperation for referrals and removal orders

De-confliction

- Avoid interference with national investigations

- Reporting
- Analysis
- Oversight and scrutiny

BENEFITS FOR HSP

Streamlining

- Centralized receipt of Removal Orders and Referrals
- Avoidance of duplication

Authentication

- Single point of contact in the context of referrals and removal orders for the EU 27

Automation

- API connection
- Feedback to MS
- Sharing of information in threat to life situations

- Reporting
- Analysis
- Scrutiny requests

03 NOV 2022
Transparency
Document made partially accessible
PUBLIC

TCO IMPLEMENTATION

Covered in PERCI

- Transmission of Removal Orders (Ar. 3-4)
- Referrals (Rec. 40)
- De-confliction, coordination (Ar. 14, par. 1)
- HSP Feedback (Ar. 3 par. 6-8)
- Reporting (Ar. 7)
- Scrutiny mechanism (Ar. 4, par. 3-7)
- 'Imminent threat to life' (Ar. 14, par. 5)

NOT Covered in PERCI

- Specific measures (ar. 5)
- Penalties (ar. 18)

PERCI State of Play

Technical implementation

- PERCI Minimum Viable Product (MVP)
- Finalising testing
- Initiated demo and trainings with MS

Document made partially available
on: 03 NOV 2021
PUBLIC

PERCI Update

PERCI Focus Group

- Working Groups on: De-confliction; Crisis response; Scrutiny process
- HSP Points of Contacts;
- Next PFG (26/9): PERCI Terms of Use; Support in interim phase; Crisis response processes;

Interim phase

- Use of IRMA for referrals;
- Deconfliction via SIENA;
- Support in crisis response (“imminent threat to life”);

Thank you for your attention

Any questions?



www.europol.europa.eu



ANEXO N.º 03: ENTREVISTA CON UN FUNCIONARIO DE LA UNIDAD DE REFERENCIA DE INTERNET DE LA UE DE EUROPOL [versión original y traducción al castellano].



COMBATING TERRORISM CENTER AT WEST POINT

CTCSENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | FEBRUARY 2020 · VOLUME 13, ISSUE 2



FEATURE ARTICLE

Fighters Without Borders

Forecasting new trends in the Iran threat
network foreign operations

MATTHEW LEVITT

A VIEW FROM THE CT FOXHOLE

Brigadier General Dagvin Anderson

COMMANDER, U.S. SPECIAL
OPERATIONS COMMAND AFRICA

Contents

FEATURE ARTICLE

1 "Fighters Without Borders"—Forecasting New Trends in Iran Threat Network Foreign Operations Tradecraft

MATTHEW LEVITT

INTERVIEWS

9 A View from the CT Foxhole: Brigadier General Dagvin R.M. Anderson, Commander, U.S. Special Operations Command Africa

JASON WARNER

15 A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit

AMARNATH AMARASINGAM

ANALYSIS

20 The Cyber Threat from Iran after the Death of Soleimani

ANNIE FIXLER

30 "Breaking the Walls" Goes Global: The Evolving Threat of Jihadi Prison Assaults and Riots

BENNETT CLIFFORD AND CALEB WEISS

FROM THE EDITOR

Following the January 3, 2020, U.S. drone strike that killed Islamic Revolutionary Guard Corps Quds Force chief General Qassem Soleimani, there is significant concern that Iran may seek to retaliate against U.S. interests in the Middle East, and possibly even in the U.S. homeland. In our feature article, Matthew Levitt forecasts that "Iran and the foreign legion of Shi'a proxies at its disposal are likely to employ new types of operational tradecraft, including deploying cells comprised of operatives from various proxy groups and potentially even doing something authorities worry about but have never seen to date, namely encouraging Shi'a homegrown violent extremist terrorist attacks."

Annie Fixler assesses Iran will likely not order a major intensification of cyber operations against the United States to avenge Soleimani per se, because "claiming credit [to make clear any attack is in retaliation] also removes plausible deniability, which is one of the benefits of cyberattacks in the first place." Instead, she argues, the state-sponsored cyber threat from Iran will continue along its current elevated trajectory, driven to a significant degree by the Iranian regime's desire to hit back because of U.S. sanctions.

Our feature interview is with Brigadier General Dagvin Anderson, Commander of U.S. Special Operations Command Africa. In our second interview, conducted by Amarnath Amarasingam, an official at Europol's EU Internet Referral Unit outlines how in November 2019, the unit coordinated with messaging platforms, including Telegram, to carry out a major takedown of Islamic State channels online.

At a time of continued concern over the security risk posed by the thousands of Islamic State fighters detained in northern Syria, Bennett Clifford and Caleb Weiss assess the global threat posed by jihadi attacks on prisons and jihadi riots inside prisons. They document how from West Africa to Southeast Asia, targeting prisons systems in this way has continued to be a priority for the Islamic State and other jihadi groups. "In planning these types of attacks," they write, "jihadis are interested in restoring their force size, releasing incarcerated jihadi leaders or specialists, and/or creating a propaganda win."

Paul Cruickshank, *Editor in Chief*

CTCSENTINEL

Editor in Chief

Paul Cruickshank

Managing Editor

Kristina Hummel

EDITORIAL BOARD

Colonel Suzanne Nielsen, Ph.D.

Department Head

Dept. of Social Sciences (West Point)

Brian Dodwell

Director, CTC

Don Rassler

Director of Strategic Initiatives, CTC

CONTACT

Combating Terrorism Center

U.S. Military Academy

607 Cullum Road, Lincoln Hall

West Point, NY 10996

Phone: (845) 938-8495

Email: sentinel@westpoint.edu

Web: www.ctc.usma.edu/sentinel/

SUBMISSIONS

The *CTC Sentinel* welcomes submissions.

Contact us at sentinel@westpoint.edu.

The views expressed in this report are those of the authors and not of the U.S. Military Academy, the Department of the Army, or any other agency of the U.S. Government.

Cover: A supporter of Lebanon's Iran-allied Hezbollah movement with a Farsi inscription reading "Revenge Severely" written on her palm, holds a picture of Qassem Soleimani, commander of the Quds Force of the Iranian Revolutionary Guard, who was killed in a U.S. airstrike in Baghdad, as she attends a mass rally and a televised speech by Hezbollah Secretary-General Hassan Nasrallah. (Marwan Naamani/picture alliance via Getty Images)

A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit

By Amarnath Amarasingam

On November 21-22, 2019, the EU Internet Referral Unit (EU IRU)—a team inside the European Union's law enforcement agency, Europol—and Telegram engaged in a serious disruption campaign against the Islamic State's channels and groups on the platform.¹ While there had been similar 'days of action' in the past, the campaign of November 2019 was far greater in scope and impact.² Hundreds of channels associated with the Islamic State-affiliated Nashir News Agency disappeared and have yet to recover.³ In this interview, which was conducted on December 11, 2019, via Skype, CTC talks with a member of the EU IRU about this campaign, about the ongoing relationship with social media companies, and the continued challenge of combating terrorist content online. The official requested anonymity. Europol has reviewed this interview and approved its publication.

CTC: What exactly is Europol's EU Internet Referral Unit? When was it founded? Was there an immediate cause that led to its founding?

Europol EU IRU Official: We set up the unit in July 2015. Within Europol, within the European Counter-Terrorism Centre (ECTC) of Europol, there was a capacity to monitor and analyze terrorist propaganda, meaning jihadist propaganda, since 2007. The scope was major jihadist groups, designated terrorist organizations. The reason for that was to have a better understanding of the threat picture, especially when it comes to the threat posed to Europe and European interests outside of Europe from these designated terrorist organizations. This was the case for some years, but then it became increasingly evident that we needed to build this capacity and also have a mandate for supporting member states with online investigations in the context of counterterrorism, plus engaging with online service providers in order to help them build their resilience against the dissemination of terrorist propaganda. So, this was the reason that the IRU was set up in 2015. And since day one, we started engaging with online service providers to flag terrorist content to them and find solutions on how to disrupt the dissemination of terrorist content online.

CTC: Were there certain social media platforms or companies that were more open to working with you from the beginning, and why do you think that was?

Europol EU IRU Official: Yeah, at that time, I recall that the bulk of the propaganda was on mainstream social media such as Twitter or Facebook. We prioritized these types of platforms to work

together, and their response was very positive. We based this on a voluntary approach. So basically, we started our operations for monitoring terrorist content—meaning content that is branded, that is produced and disseminated by designated terrorist organizations—and by tracing this content across the internet, we were in a position to also flag [it] to online service providers. So, we started flagging this type of content to the social media companies, and we engaged in a discussion with them on how we can help them improve their internal operations so they can build some measures internally to prevent the exploitation of their platforms by terrorist organizations.

CTC: Were you asking them for anything in terms of help from their side, or was it mostly you providing information to them?

Europol EU IRU Official: Our starting point is a particular media file. We don't look into particular accounts; we don't look into profiles on Facebook or Twitter accounts. We start by detecting a new media file that is put on the internet by a designated terrorist organization, and whenever we are in a position to detect and collect this content, we collect the URLs and flag the URLs to the specific post to the social media companies. Another way we help them is to share some of our experiences in, let's say, collecting visuals, logos, or markers that are used by designated terrorist organizations. We share these types of packages with them to help them understand how terrorist organizations use branding to become visible and spread their message to wider audiences.

CTC: Can you describe what a typical day looks like at the EU IRU?

Europol EU IRU Official: We are a team with people of many different backgrounds. We have the counterterrorism investigators; we have IT experts, communication experts, researchers with expertise in Islamic jurisprudence, and also in area studies. We also have linguists; we cover most of the European languages plus Arabic, Russian, and Turkish. So, we try to combine this set of skills in order to understand both the content of the message and the dissemination of the propaganda. We collect and analyze this information. There are then two lines of work. First, we support member states in their online investigations, so it's like police work, it's law enforcement work. Second, we also flag the content to the online service providers, with a request not to take down content but to review the content against their own terms of reference. Then it's up to them to make the decision whether they act upon it or not.

CTC: A number of these companies weren't always so open to acting. Why do you think there has been such a shift in culture in these social media companies more recently?⁴

Europol EU IRU Official: It was not just a shift in the understanding of social media companies, but it was a shift in the understanding of the whole international community looking at this specific issue that we cannot allow terrorist organizations to exploit publicly accessible social media and online service providers in order to promote their message, to plan their operations, to reach out to people for recruiting and financing purposes. This was crucial because we really tried to engage with the whole of the international community, not just the social media companies in doing our job. We did that in the framework of the EU Internet Forum, which was set up by the European Commission in late 2015 to facilitate this type of engagement. If I go back to this period that you mention, I can say that we have achieved at least the primary objective of restricting public access to this type of content. It's increasingly more difficult for the average user to stumble upon terrorist content as they go [about] their day-to-day browsing of the internet. Back then, a Twitter user might have been following a popular hashtag and in his Twitter feed terrorist content popped up. We thought that this was problematic, and in our discussions with social media companies, everyone agreed.

Moving forward to today, terrorist content is, of course, still accessible on the internet. We never claimed that our job is to clean the internet of terrorist content, but our job is to try to identify who is behind that, to attribute the terrorist offenses to those who are behind the screens, and also to protect the general public.

CTC: So, on the social media side you're concerned with limiting visibility. On the law enforcement side, do you only help with cases that member states come to you with, or do you proactively point them toward citizens or somebody who's in their country that they should be looking at?

Europol EU IRU Official: When it comes to investigations, we support member states with publicly available information. We don't have access to closed information. Member states need to use their legal instruments in order to request access to this type of information from the social media companies. So basically, if there's an open investigation by member states and they get access to this type of content, they can come to us for further analysis. But we don't have the legal basis to request social media companies to disclose any non-publicly available data to us.

CTC: So you're collecting data, and if law enforcement of a member state comes to you through legitimate channels, you then have the ability to help.

Europol EU IRU Official: Exactly.

CTC: How do you deal with the support network or the 'fanboys' who are very much online? Do you see official releases and supporter releases as kind of the same thing as long as they're branded, or do you deal with them differently?

Europol EU IRU Official: As long as it is branded, it is part of our concern, but of course we make a clear distinction because you cannot weigh an official statement or piece of propaganda the same way with a banner or something that is produced by a fanboy, which is not connected to jihadist media outlets. But we see this as a joint effort that has to be done by other stakeholders, by other partici-

pants in this work against terrorist content. So, we engage also with researchers; we have set up an advisor network. We try to share our experience but also to integrate the results of their research, and these discussions about how we deal with supporter-generated content is a critical issue because we see that sometimes content that is produced by just fanboys might hit the headlines, might be reproduced, and this distorts the terrorist threat assessment. It might be reproduced by people who inadvertently want to report on this content, but at the same time, they help in amplifying this content.

So, we work together with institutions, researchers, in order to raise awareness about these issues. For example, when we see that some journalists or researchers use the same hashtags [created by jihadi media outlets to promote their content] or part of a terrorist video clip to report on the terrorist content, we can see this as problematic because at the same time, you reproduce or you further spread this message. The point here is that unedited content or content that re-mediatizes the brand of the terrorist organization should not be circulated. Most professionals take a nuanced approach, but this is not always the case. So again, we have an extended network of stakeholders; we work with European institutions, with European Strategic Communication Network (ESCN), with the Radicalization Awareness Network (RAN), with the global research network that was set up by the Global Internet Forum to Counter Terrorism (GIFCT).

CTC: What surprised you most about how the Islamic State has used the internet as compared to other terrorist groups?

Europol EU IRU Official: The first thing that comes to my mind is their branding, how they were able to promote and maintain their branding. From a researcher's point of view, from someone who is engaging with terrorist content, you see that IS had to put up with changes many times in the past. They had to change their narrative from the apocalyptic discourse, Dabiq and the end of days battle, and "remaining and expanding." Then they lose territory, but still they remain relevant by continuously changing their narrative. They ask their supporters to remain steadfast and so on. For me, there were many missed opportunities. I would have expected the impact of them having to change the discourse so many times to have been more negative than it was. Because they were able to maintain the branding and basically create an online environment that took on its own life and was somehow disconnected from the reality on the ground, this was something that in my view was problematic and this is where we need to focus more.

CTC: When the Islamic State started to move to Telegram in late 2015, how did that impact your work?⁵

Europol EU IRU Official: As I said, we start our observations from tracing content. So, when they moved to Telegram, we tried to reach out to Telegram and explain the situation. We started flagging terrorist content to Telegram, and gradually we established a channel of communication and cooperation with Telegram. For tech companies, when they set up their own business, they don't think about the exploitation of their platform by terrorists. So for many companies, not just for Telegram, the first step is to raise awareness about what's happening on their platform and then start building trust with them. This is important, and that's why we highlight the importance of voluntary cooperation, the importance of the public/

private partnership. If I'm being honest, some of the online service providers that we try to engage with, their first reaction is why is a law enforcement agency asking me to review this type of content? What is behind that? Do you come with a legal mandate? Are you going to ask for more information? We [Europol] don't have any enforcement powers there. Our legal mandate is to flag the content and then work together with them [social media companies] to raise awareness. Then it's their own decision. This is also how it worked with Telegram.

CTC: There is a perception that Telegram was slow in the beginning to come to the table. What do you think the reason for that was?⁶

Europol EU IRU Official: I cannot say whether it was slow or fast, but it takes time until tech companies understand what the problem is. What is important is for us to maintain this type of communication, to establish regular communication, and try to engage and give the right answers to these companies. Not everyone wants to engage; in some cases, they're not interested and then they don't engage.

CTC: Why do you think that kind of shift happened for Telegram?

Europol EU IRU Official: I think it's partly that they realized that they don't need to put up anymore with this type of activity. No online service provider would have ever liked to put up with this type of activity. And if you see the joint press release that we have published on our website, in the aftermath of the Europol campaign, there's also a quote from Telegram saying basically that enough is enough.⁷ They see this as their responsibility, to have a platform that is free of terrorist abuse.

CTC: Can you describe the November 2019 operation Europol coordinated with online communication platforms such as Telegram to take down Islamic State content?⁸

Europol EU IRU Official: This was part of our standard procedure in engaging with online service providers. We had already done a couple of, let's say, actions together with Telegram in the past. We cover a large number of online service providers, not just Telegram. But at some point last year, we took some time to specifically look at Telegram. We did a joint action, and then we started building from that point on into trying to work closer together to map the network of core disseminators, so to speak, propagandists whose main business it is to disseminate this type of content. And this cooperation culminated with this type of action, but at the same time, we have been working together with law enforcement in member states in order to disrupt the internet operations of the Islamic state. In the past, we did some investigative work, and together with the prosecutors, we managed to cease some of the web assets (e.g., servers) that the Islamic State propagandists were using to store content [and] to communicate.

And these actions we saw as opportune [in their] timing. We did not merge the two actions, but wanted to have an impact by using the time factor there. So the prosecutors, member state investigators working on the investigative part, and then also content specialists, referral specialists, working with Telegram and other

platforms to refer this type of content. This was a planned action, and we knew that if this went well, it would shake up the community of jihadist propagandists on Telegram.

And by disrupting their operations on Telegram, you create new opportunities [for those working on counterterrorism]. I mean, it was not that difficult to guess what they would try next. Of course, we don't know everything, but there were already some indications from 2018 that they were willing to experiment with certain platforms. It was not a big surprise that they tried to go back and use some of these platforms. They, of course, experimented with some new platforms, but this creates a lot of opportunities [for those working on counterterrorism]. First of all, this creates a lot of disruption. Then it has an impact on the branding, because nobody's sure who is creating the new channels, the new Nashir channels, the new Amaq channels, on each new platform. What is the message? We see now many messages that caution protagonists or sympathizers from using this or the other platform or using or following this or the other media outlet. So, there's a clear impact on brand, and there's also an opportunity to create new investigative leads.

So, what I'm saying here is that in the past, we worked on both the investigation/attribution and the referral aspects. But now we try to bridge the gap there. So, this is not the end of the story. This is the beginning of the story, and that's why we really want to engage with the international community to put all of our efforts together to work both on prevention and attribution. By disrupting the jihadist networks on the internet, you contribute to prevention. This is what we're trying to do here by doing referrals; by flagging this content in a timely manner to online service providers and by helping member states to investigate these networks, we try to bridge the gap that we've seen in the past between prevention and investigative work.

CTC: That part of it is especially interesting. Are you seeing social media companies being open to working with member states, and are you trying to serve as the bridge between those two?

Europol EU IRU Official: Yes, absolutely. And as I already mentioned, there's now an understanding among social media companies that they shouldn't put up with this type of exploitation. Again, this depends on the platform and on their relationship with investigators and prosecutors in member states. We see that some platforms are more willing than others to share additional information. This has nothing to do with freedom of speech. We are, of course, for the protection of freedom of speech and fundamental rights and the digital rights of citizens, but our focus is very targeted. And we see that companies start seeing this as another type of crime around which they have already been working with law enforcement, like banking fraud or child sexual exploitation. They're willing to share more data because they see a benefit from disrupting these networks and bringing these people to justice.

CTC: The Europol press release mentioned that the November 2019 operation "was led by the Belgian Investigating Counter Terrorism Judge and the Belgian Federal Prosecutor's Office, together with the Belgian Federal Judicial Police of East-Flanders." And there is mention of "an arrest in Spain of an individual suspected of being part of the core disseminators of IS terrorist propaganda online."⁹ What is the significance of men-

tioning these law enforcement agencies in the press release?

Europol EU IRU Official: This is related to the operational work. Member states were working together with us to seize some of the assets and create some investigative leads. This phase of the operation—I'm talking about the investigative part, not the referral part—was led by the Belgian prosecuting authorities, and the Belgian and the Spanish colleagues wanted to present a strong message that this is the way forward. All of us getting together, working together in order to attribute terrorist offenses to the perpetrators.

CTC: Some people say that what you and others are doing is basically just a game of cat and mouse—just chasing terrorists around the internet. They say that this is not a good use of law enforcement time and energy. How do you respond to that?

Europol EU IRU Official: I would like to go a few years back and compare the situation today with the situation back in 2014, 2015. I think it's unfair to say that there's no progress made in this respect. Now, I see that the focus is on this whack-a-mole game, but we're talking about a steep decrease in terrorist propaganda output, especially high-profile items coming from the officially endorsed media outlets. Today, we're talking about some networks of people who really want to exploit small- and medium-sized enterprises online to disseminate terrorist content and especially supporter-generated content. But this is limited. This is more limited than it used to be back in 2015, 2016. So, if we want to be fair, I think we have to give some credit to this effort, to the public/private partnership that has been put forward since that time and recognize that now we're dealing with a different kind of problem. Of course, some people are dedicated disseminators and supporters of these organizations. The internet is an enabler; it's not the root cause of terrorism. But we need to take some action because otherwise you just leave it open to whoever wants to exploit the situation.

CTC: Can you talk a little bit about the Islamic State media structure, what you noticed with their presence in Syria and Iraq versus Europe or North America? Were there core individuals everywhere, or was it centered in Syria and Iraq? And relatedly, how did the destruction of the physical caliphate impact the media environment and structure?

Europol EU IRU Official: This is a very difficult question. What I can say is that we think that there are different layers of the structure they have put forward to produce and disseminate content. At the peak of their activity, they have styled Amaq as like an independent news agency to report on the evolution on the ground in real time. At the same time, they had the officially endorsed media outlets. Then there was another layer of supporting media outlets; some of them pre-dated the advent of the Islamic state, and they pledged allegiance to the Islamic State. Some others were created to support the work of the Islamic State, but they, at the same time, produced their own content and disseminated their own content.

And then in the third layer, there were sympathizers who were willing to create the supporter-generated content and disseminate it. So, we give different weights to these layers.

Also, at the peak of their activity, they used to have a very sophisticated campaign on the internet starting from sending out teasers about new releases, like about the magazines they were going to put out. This was what we thought of as the “seeding phase.” Then there was the “launch phase,” and then they had the “echo phase” in which they re-mediatized content in large volumes. This was a sophisticated campaign on their side when it comes to strategic communications, and this has also been the target of our operations. By doing that, and working together with member states and law enforcement, you come across valuable information, and I think that over the past years, member states, law enforcement, and judicial services have managed to disrupt part of this network and bring these people to justice. This is a continuous effort, a work in progress.

CTC: I've observed in my research how university students have helped translate material for the Islamic State and build banners and so on. To what degree are younger people joining the media apparatus post 2018/2019?¹⁰

Europol EU IRU Official: I'm afraid I cannot talk about the demographics because we don't have any specific analysis on that. But, for us, it's important to continue working with law enforcement and member states. They're responsible for the investigations, and they're responsible for dealing with those joining the terrorist organization in their effort to propagate their narratives. We also want to share our experience with other institutions. I mentioned, for example, the Radicalization Awareness Network because prevention is equally important. We are a counterterrorism center and we deal with counterterrorism, but I think that our experience is valuable for others who work on the prevention side. So, we try to engage, we try to share our experience and our knowledge, and we hope that the root causes of terrorism are addressed and that preventive work is done to stop people from resorting to this type of activity.

CTC: Is your team involved on the far-right side of things as well? There's a lot of far-right activity on Telegram and other platforms. Are you also looking at that and other kind of ideologically inspired terrorist violence, or is it mostly focused on jihadi material?

Europol EU IRU Official: So far it has been mostly focused on jihadi terrorist propaganda. In some cases, we also supported member states in far-right terrorist cases. This is basically under discussion currently to see how Europol can further support this effort in other fields. Of course, there's some similarities but also some differences when we talk about right-wing terrorist groups. So, we're currently looking into that, to assess how we can better contribute to this effort. **CTC**

Citations

- 1 "Europol and Telegram Take on Terrorist Propaganda Online," Europol, November 25, 2019.
- 2 "Europol disrupts Islamic State propaganda machine," BBC Monitoring, November 25, 2019.
- 3 Ibid. See also "Jihadists Presence Online Decentralizes After Telegram Ban," Flashpoint, January 17, 2020; tracking of Islamic State-associated online content by the author (Amarnath Amarasingam).
- 4 Jessica Stern and J.M. Berger, *ISIS: The State of Terror* (New York: Harper Collins, 2015), p. 134.
- 5 "Jihadis Shift to Using Secure Communication App Telegram's Channel Service," MEMRI, October 29, 2015.
- 6 For analysis of the Islamic State's previous presence on Telegram, see Bennett Clifford, "'Trucks, Knives, Bombs, Whatever': Exploring Pro-Islamic State Instructional Material on Telegram," *CTC Sentinel* 11:5 (2018); Bennett Clifford and Helen Powell, "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram," George Washington University's Program on Extremism, June 2019; Laurence Binder, "Wilayat Internet: ISIS's Resilience Across the Internet and Social Media," Bellingcat, September 1, 2017.
- 7 Editor's note: "Europol and Telegram Take on Terrorist Propaganda Online."
- 8 Ibid.; Paolo Zialcita, "Islamic State's 'Not Present on the Internet Any-more' Following European Operation," NPR, November 25, 2019.
- 9 "EU Law Enforcement and Judicial Authorities Join Forces to Disrupt Terrorist Propaganda Online," Europol, November 25, 2010.
- 10 Amarnath Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For," Vice Motherboard, December 5, 2019.

Traducción de Gilda B. Gadea Aldave de la entrevista: Europol EU IRU Official (2020). *A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit* / Entrevistado por A. Amarasingam. CTC Sentinel, Combating Terrorism Center at West Point (CTC). (p. 15). Disponible en Internet en: <https://ctc.westpoint.edu/view-ct-foxhole-interview-official-europols-eu-internet-referral-unit/>

UNA VISIÓN DESDE LA TRINCHERA DE CT: UNA ENTREVISTA CON UN FUNCIONARIO DE LA UNIDAD DE REFERENCIA DE INTERNET DE LA UE DE EUROPOL

FEBRERO 2020, VOLUMEN 13, NÚMERO 2

Autor:

AMARNATH AMARASINGAM

El 21 y 22 de noviembre de 2019, la Unidad de Referencia de Internet de la UE (EU IRU, por sus siglas en inglés)—un equipo dentro de la agencia policial de la Unión Europea, Europol—y Telegram participaron en una seria campaña de interrupción contra los canales y grupos del Estado Islámico en la plataforma. Si bien hubo “días de acción” similares en el pasado, la campaña de noviembre de 2019 fue mucho mayor en alcance e impacto. Cientos de canales asociados con la Agencia de Noticias Nashir, afiliada al Estado Islámico, desaparecieron y aún no se han recuperado. En esta entrevista, que se realizó el 11 de diciembre de 2019 a través de Skype, CTC habla con un miembro de la EU IRU sobre esta campaña, sobre la relación actual con las empresas de redes sociales y el desafío continuo de combatir el contenido terrorista en línea. El funcionario solicitó el anonimato. Europol ha revisado esta entrevista y ha aprobado su publicación.

CTC: ¿Qué es exactamente la Unidad de Referencia de Internet de la UE de Europol? ¿Cuándo fue fundada? ¿Hubo una causa inmediata que llevó a su fundación?

Oficial de Europol EU IRU: Creamos la unidad en julio de 2015. Dentro del Centro Europeo Contra el Terrorismo (ECTC) de Europol, había capacidad para monitorear y analizar la propaganda terrorista, es decir, la propaganda yihadista, desde 2007. El alcance eran grandes grupos yihadistas, organizaciones terroristas designadas. La razón de esto fue tener una mejor comprensión del panorama de amenazas, especialmente cuando se trata de la amenaza que representan estas organizaciones designadas como terroristas para Europa, y los intereses europeos fuera de Europa. Este fue el caso durante algunos años, pero luego se hizo cada vez más evidente que necesitábamos desarrollar esta capacidad y también tener un mandato para apoyar a los Estados miembros con investigaciones en línea en el contexto de la lucha contra el terrorismo, además de colaborar con los proveedores de servicios en línea para ayudarlos. desarrollar su resiliencia contra la difusión de propaganda terrorista. Entonces, esta fue la razón por la que se creó la IRU en 2015. Y desde el primer día, comenzamos a colaborar con proveedores de servicios en línea para señalarles contenido terrorista y encontrar soluciones sobre cómo interrumpir la difusión de contenido terrorista en línea.

CTC: ¿Hubo plataformas de redes sociales o empresas que estuvieron más abiertas a trabajar con vosotros desde el principio y por qué cree que fue así?

Oficial de Europol EU IRU: Sí, en ese momento, recuerdo que la mayor parte de la propaganda estaba en las principales redes sociales como Twitter o Facebook. Priorizamos este tipo de plataformas para trabajar juntas y su respuesta fue muy positiva. Basamos esto en un enfoque voluntario. Básicamente, comenzamos nuestras operaciones para monitorear contenido terrorista, es decir, contenido de marca, producido y difundido por organizaciones terroristas designadas, y al rastrear este contenido a través de Internet, estábamos en condiciones de señalarlo también en línea. Entonces, comenzamos a señalar este tipo de contenido a las empresas de redes sociales y entablamos una discusión con ellas sobre cómo podemos ayudarlos a mejorar sus operaciones internas para que puedan desarrollar algunas medidas para prevenir la explotación de sus plataformas por parte de organizaciones terroristas.

CTC: ¿Se le estaba pidiendo algo en términos de ayuda [a las empresas], o principalmente erais vosotros quien les proporcionabas información?

Oficial de Europol EU IRU: Nuestro punto de partida es un archivo multimedia particular. No analizamos cuentas particulares. No miramos perfiles en cuentas de Facebook o Twitter. Comenzamos detectando un nuevo archivo multimedia que una organización terrorista designada coloca en Internet y, siempre que estamos en condiciones de detectar y recopilar este contenido, recopilamos las URL y marcamos las URL de la publicación específica en las redes sociales. Otra forma en que los ayudamos es compartiendo algunas de nuestras experiencias, digamos, recopilando imágenes, logotipos o marcadores que utilizan organizaciones terroristas designadas. Compartimos este tipo de paquetes con ellos para ayudarlos a comprender cómo las organizaciones terroristas utilizan la marca para hacerse visibles y difundir su mensaje a audiencias más amplias.

CTC: ¿Puedes describir cómo es un día típico en la IRU de la UE?

Oficial de Europol EU IRU: Somos un equipo con personas de diferentes orígenes. Tenemos a los investigadores antiterroristas. Contamos con expertos en TI, expertos en comunicación, investigadores con experiencia en jurisprudencia islámica y también en estudios de área. También tenemos lingüistas. Cubrimos la mayoría de los idiomas europeos además de árabe, ruso y turco. Así, intentamos combinar este conjunto de habilidades para comprender tanto el contenido del mensaje como la difusión de la propaganda. Recopilamos y analizamos esta información. Hay entonces dos líneas de trabajo. En primer lugar, apoyamos a los Estados miembros en sus investigaciones en línea, por lo que es como trabajo policial, es trabajo de aplicación de la ley. En segundo lugar, también señalamos el contenido a los proveedores de servicios en línea, solicitándoles que no eliminen el contenido, sino que lo revisen según sus propios términos de referencia. Entonces depende de ellos tomar la decisión de actuar en consecuencia o no.

CTC: Varias de estas empresas no siempre estuvieron tan abiertas a actuar. ¿Por qué crees que ha habido tal cambio cultural en estas empresas de redes sociales más recientemente?

Oficial de Europol EU IRU: No fue solo un cambio en la comprensión de las empresas de redes sociales, sino que fue un cambio en la comprensión de toda la comunidad internacional que analiza este tema específico. No podemos permitir que las organizaciones terroristas exploten las redes sociales de acceso público y proveedores de

servicios en línea para promover su mensaje, planificar sus operaciones y llegar a las personas con fines de reclutamiento y financiación. Esto fue crucial porque realmente intentamos involucrarnos con toda la comunidad internacional, no solo con las empresas de redes sociales, para hacer nuestro trabajo. Lo hicimos en el marco del Foro de Internet de la UE, creado por la Comisión Europea a finales de 2015 para facilitar este tipo de participación. Si vuelvo a este periodo que mencionas, puedo decir que hemos conseguido al menos el objetivo principal de restringir el acceso público a este tipo de contenidos. Cada vez es más difícil para el usuario promedio tropezar con contenido terrorista mientras navega diariamente por Internet. En aquel entonces, un usuario de Twitter podría haber estado siguiendo un hashtag popular y en su cuenta de Twitter aparecía contenido terrorista. Pensamos que esto era problemático y, en nuestras conversaciones con las empresas de redes sociales, todos estuvieron de acuerdo.

El contenido terrorista, por supuesto, sigue siendo accesible en Internet. Nunca dijimos que nuestro trabajo sea limpiar Internet de contenido terrorista, nuestro trabajo es tratar de identificar quién está detrás de eso, atribuir los delitos terroristas a quienes están detrás de las pantallas y también proteger al público en general.

CTC: Entonces, en lo que respecta a las redes sociales, lo que preocupa es limitar la visibilidad. En lo que respecta a las fuerzas del orden, ¿solo ayudan con los casos que los Estados miembros les presentan, o les dirigen de manera proactiva hacia ciudadanos o alguien que está en su país a quien deberían estar investigando?

Oficial de Europol EU IRU: Cuando se trata de investigaciones, apoyamos a los Estados miembros con información pública disponible. No tenemos acceso a información cerrada. Los Estados miembros deben utilizar sus instrumentos legales para solicitar acceso a este tipo de información a las empresas de redes sociales. Básicamente, si hay una investigación abierta por parte de los Estados miembros y obtienen acceso a este tipo de contenido, pueden acudir a nosotros para realizar un análisis más detallado. Pero no tenemos la base legal para solicitar a las empresas de redes sociales que nos revelen datos que no estén disponibles públicamente.

CTC: Entonces, recopilan datos. Y por otra parte, si las autoridades de un Estado miembro llegan a vosotros a través de investigaciones judiciales, entonces tienes la capacidad de ayudar?

Oficial de Europol EU IRU: Exactamente.

CTC: ¿Cómo manejas la red de apoyo o los ‘fanboys’ que están mucho en línea? ¿Consideras que los lanzamientos oficiales y los de los seguidores son lo mismo siempre que tengan una marca, o los tratas de manera diferente?

Oficial de Europol EU IRU: Siempre que tenga una marca, es parte de nuestra preocupación, pero por supuesto hacemos una distinción clara porque no se puede comparar una declaración oficial o una pieza de propaganda de la misma manera con una pancarta o algo producido por un fanboy, que no está relacionado con los medios de comunicación yihadistas. Pero consideramos que esto es un esfuerzo conjunto que deben realizar otras partes interesadas, otros participantes en este trabajo contra el contenido terrorista. Por eso, también colaboramos con los investigadores. Hemos creado una red de asesores. Intentamos compartir nuestra experiencia, pero también integrar los resultados de su investigación, y estas discusiones sobre cómo manejamos el contenido

generado por los seguidores es un tema crítico porque vemos que a veces el contenido producido solo por fanáticos puede aparecer en los titulares, puede reproducirse, lo que distorsiona la evaluación de la amenaza terrorista. Puede ser reproducido por personas que sin darse cuenta quieren informar sobre este contenido, pero al mismo tiempo ayudan a amplificar este contenido.

Entonces, trabajamos en conjunto con instituciones, investigadores, para generar conciencia sobre estos temas. Por ejemplo, cuando vemos que algunos periodistas o investigadores utilizan los mismos hashtags [creados por medios yihadistas para promocionar su contenido] o parte de un videoclip terrorista para informar sobre el contenido terrorista, podemos verlo como problemático porque al mismo tiempo vez, reproduces o difundes este mensaje. El punto aquí es que no debe circular contenido sin editar o contenido que publicite la marca de la organización terrorista. La mayoría de los profesionales adoptan un enfoque matizado, pero no siempre es así. Una vez más, contamos con una red amplia de partes interesadas. Trabajamos con instituciones europeas, con la Red Europea de Comunicación Estratégica (ESCN), con la Red de Concientización sobre la Radicalización (RAN), con la Red Global de Investigación creada por el Foro Global de Internet para Contrarrestar el Terrorismo (GIFCT).

CTC: ¿Qué es lo que más le sorprendió acerca de cómo el Estado Islámico ha utilizado Internet en comparación con otros grupos terroristas?

Oficial de Europol EU IRU: Lo primero que me viene a la mente es su marca, cómo pudieron promover y mantener su marca. Desde el punto de vista de un investigador, de alguien que se involucra con contenido terrorista, se ve que el EI tuvo que soportar cambios muchas veces en el pasado. Tuvieron que cambiar su narrativa del discurso apocalíptico (Dabiq y la batalla del fin de los días), y “permanecer y expandirse”. Luego pierden territorio, pero siguen siendo relevantes al cambiar continuamente su narrativa. Piden a sus seguidores que se mantengan firmes y así sucesivamente. Para mí, hubo muchas oportunidades perdidas. Habría esperado que el impacto de que tuvieran que cambiar el discurso tantas veces hubiera sido más negativo de lo que fue. Debido a que fueron capaces de mantener la marca y básicamente crear un entorno en línea que cobró vida propia y de alguna manera estaba desconectado de la realidad sobre el terreno, esto fue algo que, en mi opinión, fue problemático y aquí es donde debemos centrarnos más.

CTC: Cuando el Estado Islámico comenzó a migrar a Telegram a finales de 2015, ¿cómo afectó eso a su trabajo?

Oficial de Europol EU IRU: Como dije, comenzamos nuestras observaciones rastreando el contenido. Entonces, cuando se mudaron a Telegram, intentamos comunicarnos con Telegram y explicar la situación. Comenzamos a señalar contenido terrorista en Telegram y gradualmente establecimos un canal de comunicación y cooperación con Telegram. Las empresas de tecnología, cuando crean su propio negocio, no piensan en la explotación de su plataforma por parte de terroristas. Entonces, para muchas empresas, no solo para Telegram, el primer paso es generar conciencia sobre lo que sucede en su plataforma y luego comenzar a generar confianza con ellas. Esto es importante y por eso destacamos la importancia de la cooperación voluntaria, la importancia de la asociación público-privada. Si soy honesto, algunos de los proveedores de servicios en línea con los que intentamos interactuar, su primera reacción es ¿por qué una agencia policial me pide que revise este tipo de contenido? ¿Qué hay detrás de eso? ¿Vienes con mandato legal? ¿Vas a pedir más información? Nosotros [Europol] no tenemos ningún poder de ejecución allí.

Nuestro mandato legal es marcar el contenido y luego trabajar junto con ellas [las empresas de redes sociales] para crear conciencia. Entonces es su propia decisión. Así también funcionó con Telegram.

CTC: Existe la percepción de que Telegram tardó al principio en llegar a la mesa de trabajo. ¿Cuál crees que fue la razón de eso?

Oficial de Europol EU IRU: No puedo decir si fue lento o rápido, pero lleva tiempo hasta que las empresas de tecnología comprendan cuál es el problema. Lo importante para nosotros es mantener este tipo de comunicación, establecer una comunicación regular e intentar involucrarnos y dar las respuestas correctas a estas empresas. No todo el mundo quiere participar; en algunos casos, no están interesados y no participan.

CTC: ¿Por qué crees que ocurrió ese tipo de cambio en Telegram?

Funcionario de Europol EU IRU: Creo que en parte es porque se dieron cuenta de que no necesitan aguantar más este tipo de actividad. A ningún proveedor de servicios en línea le hubiera gustado tolerar este tipo de actividad. Y si observan el comunicado de prensa conjunto que publicamos en nuestro sitio web, después de la campaña de Europol, también hay una cita de Telegram que dice básicamente que ya es suficiente. Consideran que es su responsabilidad tener una plataforma que está libre de abusos terroristas.

CTC: ¿Puede describir la operación de noviembre de 2019 que Europol coordinó con plataformas de comunicación en línea como Telegram para eliminar el contenido del Estado Islámico?

Oficial de Europol EU IRU: Esto era parte de nuestro procedimiento estándar al relacionarnos con proveedores de servicios en línea. Ya habíamos realizado un par de, digamos, acciones junto con Telegram en el pasado. Cubrimos una gran cantidad de proveedores de servicios en línea, no solo Telegram. Pero en algún momento del año pasado, nos tomamos un tiempo para analizar específicamente Telegram. Hicimos una acción conjunta y luego comenzamos a construir a partir de ese momento para tratar de trabajar más estrechamente para mapear la red de diseminadores centrales, por así decirlo. Propagandistas cuyo negocio principal es difundir este tipo de contenido. Y esta cooperación culminó con este tipo de acción, pero al mismo tiempo, hemos estado trabajando junto con las Fuerzas del orden en los Estados miembros para interrumpir las operaciones en Internet del Estado Islámico. En el pasado, hicimos algún trabajo de investigación y, junto con los fiscales, logramos interrumpir algunos de los activos web (por ejemplo, servidores) que los propagandistas del Estado Islámico estaban usando para almacenar contenido y comunicarse.

Y estas acciones las consideramos oportunas en su momento. Esta fue una acción planificada y sabíamos que, si salía bien, sacudiría a la comunidad de propagandistas yihadistas en Telegram.

Al interrumpir sus operaciones en Telegram, se crean nuevas oportunidades [para quienes trabajan en contrterrorismo]. Quiero decir, no fue tan difícil adivinar qué intentarían a continuación. Por supuesto, no lo sabemos todo, pero ya desde 2018 hubo algunos indicios de que estaban dispuestos a experimentar con determinadas plataformas. No fue una gran sorpresa que intentaran volver atrás y utilizar algunas de estas plataformas. Por supuesto, experimentaron con algunas plataformas nuevas, pero esto crea muchas oportunidades [para quienes trabajan en contrterrorismo]. En primer lugar, esto crea

muchas perturbaciones. Luego tiene un impacto en la marca, porque nadie está seguro de quién está creando los nuevos canales, los nuevos canales Nashir, los nuevos canales Amaq, en cada nueva plataforma. ¿Cuál es el mensaje? Vemos ahora muchos mensajes que advierten a los protagonistas o simpatizantes de usar esta u otra plataforma o usar o seguir este u otro medio de comunicación. Por lo tanto, hay un claro impacto en la marca y también existe la oportunidad de crear nuevas pistas de investigación.

Entonces, lo que estoy diciendo aquí es que en el pasado trabajamos tanto en los aspectos de investigación/atribución como en los de remisión. Pero ahora intentamos cerrar la brecha allí. Entonces, este no es el final de la historia. Este es el comienzo de la historia y es por eso por lo que realmente queremos involucrarnos con la comunidad internacional para unir todos nuestros esfuerzos para trabajar tanto en la prevención como en la atribución. Al dismantelar las redes yihadistas en Internet, se contribuye a la prevención. Esto es lo que intentamos hacer aquí al hacer referencias; Al señalar este contenido de manera oportuna a los proveedores de servicios en línea y al ayudar a los estados miembros a investigar estas redes, intentamos cerrar la brecha que hemos visto en el pasado entre la prevención y el trabajo de investigación.

CTC: Esa parte es especialmente interesante. ¿Ves que las empresas de redes sociales están abiertas a trabajar con los Estados miembros?, y ¿Están tratando de servir como puente entre esos dos?

Oficial de Europol EU IRU: Sí, absolutamente. Y como ya mencioné, ahora existe un entendimiento entre las empresas de redes sociales de que no deberían tolerar este tipo de explotación. Una vez más, esto depende de la plataforma y de su relación con los investigadores y fiscales de los Estados miembros. Vemos que algunas plataformas están más dispuestas que otras a compartir información adicional. Esto no tiene nada que ver con la libertad de expresión. Por supuesto, estamos a favor de la protección de la libertad de expresión y los derechos fundamentales y los derechos digitales de los ciudadanos, pero nuestro enfoque es muy específico. Y vemos que las empresas empiezan a ver esto como otro tipo de delito en torno al cual ya han estado trabajando con las autoridades, como el fraude bancario o la explotación sexual infantil. Están dispuestos a compartir más datos porque ven un beneficio en interrumpir estas redes y llevar a estas personas ante la justicia.

CTC: Un comunicado de prensa de Europol menciona que la operación de noviembre de 2019 “fue dirigida por el juez de investigación antiterrorista belga y la Fiscalía Federal belga, junto con la Policía Judicial Federal belga de Flandes Oriental”. Y se menciona “un arresto en España de un individuo sospechoso de ser parte de los principales difusores de propaganda terrorista del EI en línea”. ¿Cuál es el significado de mencionar a estos organismos encargados de hacer cumplir la ley en el comunicado de prensa?

Oficial de Europol EU IRU: Esto está relacionado con el trabajo operativo. Los Estados miembros estaban trabajando junto con nosotros para confiscar algunos de los activos y crear algunas pistas de investigación. Esta fase de la operación (me refiero a la parte de investigación, no a la de remisión) fue dirigida por las autoridades judiciales belgas, y los colegas belgas y españoles querían presentar un mensaje contundente de que éste es el camino por seguir. Todos nos unimos, trabajamos juntos para atribuir los delitos terroristas a los perpetradores.

CTC: Algunas personas dicen que lo que vuestra unidad y otros están haciendo es básicamente un juego del gato y el ratón: simplemente perseguir terroristas por Internet. Dicen que este no es un buen uso del tiempo y la energía de las Fuerzas del orden. ¿Como responde a eso?

Funcionario de Europol EU IRU: Me gustaría retroceder unos años y comparar la situación actual con la situación de 2014 o 2015. Creo que es injusto decir que no se han logrado avances en este sentido. Ahora, veo que la atención se centra en este juego de “golpear al topo” [*expresión que se utiliza con referencia a una situación en la que los intentos de resolver un problema son poco sistemáticos o superficiales, y dan como resultado sólo una mejora temporal o menor*], pero estamos hablando de una fuerte disminución en la producción de propaganda terrorista, especialmente artículos de alto perfil provenientes de los medios de comunicación respaldados oficialmente. Hoy estamos hablando de algunas redes de personas que realmente quieren explotar a las pequeñas y medianas empresas en línea para difundir contenido terrorista y, especialmente, contenido generado por seguidores. Pero esto es limitado. Esto es más limitado de lo que solía ser en 2015 o 2016. Entonces, si queremos ser justos, creo que tenemos que darle algo de crédito a este esfuerzo, a la asociación público-privada que se ha presentado desde entonces, y reconocer que ahora nos enfrentamos a un tipo diferente de problema. Por supuesto, algunas personas son dedicados divulgadores y partidarios de estas organizaciones. Internet es un facilitador; no es la causa fundamental del terrorismo. Pero tenemos que tomar algunas medidas porque, de lo contrario, se deja abierta la posibilidad a quien quiera explotar la situación.

CTC: ¿Puedes hablar un poco sobre la estructura mediática del Estado Islámico, lo que notaste con su presencia en Siria e Irak versus Europa o América del Norte? ¿Había individuos centrales en todas partes o se centraba en Siria e Irak? Y en relación con esto, ¿cómo afectó la destrucción del califato físico al entorno y la estructura de los medios?

Europol EU IRU Oficial: Esta es una pregunta muy difícil. Lo que puedo decir es que pensamos que hay diferentes capas de la estructura que han propuesto para producir y difundir contenidos. En el apogeo de su actividad, han diseñado a Amaq como una agencia de noticias independiente para informar sobre la evolución sobre el terreno en tiempo real. Al mismo tiempo, contaban con los medios de comunicación avalados oficialmente. Luego hubo otra capa de medios de comunicación de apoyo. Algunos de ellos son anteriores al advenimiento del Estado Islámico y juraron lealtad al Estado Islámico. Algunos otros fueron creados para apoyar el trabajo del Estado Islámico, pero, al mismo tiempo, produjeron su propio contenido y difundieron su propio contenido. Y luego, en la tercera capa, había simpatizantes que estaban dispuestos a crear contenido generado por sus seguidores y difundirlo. Entonces, le damos diferentes pesos a estas capas.

Además, en el pico de su actividad, solían tener una campaña muy sofisticada en Internet que comenzaba con el envío de teasers sobre nuevos lanzamientos, como sobre las revistas que iban a sacar. Esto era lo que pensábamos que era la “fase de siembra”. Luego estuvo la “fase de lanzamiento” y luego tuvieron la “fase de eco” en la que publicitaron contenido en grandes volúmenes. Esta fue una campaña sofisticada de su parte en lo que respecta a comunicaciones estratégicas, y este también ha sido el objetivo de nuestras operaciones. Al hacerlo, y trabajando junto con los Estados miembros y las fuerzas del orden, se obtiene información valiosa, y creo que, en los últimos años, los Estados miembros, las fuerzas del orden y los servicios judiciales han logrado desarticular parte

de esta red y traer a estas personas a la justicia. Este es un esfuerzo continuo, un trabajo en progreso.

CTC: En mi investigación he observado cómo los estudiantes universitarios han ayudado a traducir material para el Estado Islámico y a construir pancartas, etc. ¿En qué medida los jóvenes se están incorporando al aparato mediático después de 2018/2019?

Europol EU IRU Oficial: Me temo que no puedo hablar de datos demográficos porque no tenemos ningún análisis específico al respecto. Pero para nosotros es importante seguir trabajando con las autoridades y los Estados miembros. Son responsables de las investigaciones y de tratar con quienes se unen a la organización terrorista en su esfuerzo por propagar sus narrativas. También queremos compartir nuestra experiencia con otras instituciones. Mencione, por ejemplo, la Red de Sensibilización sobre la Radicalización porque la prevención es igualmente importante. Somos un centro antiterrorista y nos ocupamos del contraterrorismo, pero creo que nuestra experiencia es valiosa para otros que trabajan en el ámbito de la prevención. Por eso, tratamos de involucrarnos, tratamos de compartir nuestra experiencia y nuestro conocimiento, y esperamos que se aborden las causas profundas del terrorismo y que se realice un trabajo preventivo para evitar que la gente recurra a este tipo de actividad.

CTC: ¿Su equipo también está involucrado en identificar las actividades de la extrema derecha? Hay mucha actividad de extrema derecha en Telegram y otras plataformas. ¿Está usted también analizando ese y otros tipos de violencia terrorista de inspiración ideológica, o se centra en el contenido yihadista?

Europol EU IRU Oficial: Hasta ahora EU IRU se ha centrado principalmente en la propaganda terrorista yihadista. En algunos casos, también apoyamos a los Estados miembros en casos de terrorismo de extrema derecha. Básicamente, esto se está debatiendo actualmente para ver cómo Europol puede seguir apoyando este esfuerzo en otros campos. Por supuesto, hay algunas similitudes, pero también algunas diferencias cuando hablamos de grupos terroristas de derecha. Actualmente estamos investigando eso para evaluar cómo podemos contribuir mejor a este esfuerzo.

ANEXO N.º 04: COMUNICADO DE PRENSA: LEY DE SERVICIOS DIGITALES:
ENTRAN EN VIGOR LAS NORMAS DETERMINANTES DE LA UE PARA LAS
PLATAFORMAS EN LÍNEA.



Ley de Servicios Digitales: entran en vigor las normas determinantes de la UE para las plataformas en línea

Bruselas, 16 de noviembre de 2022

Hoy entra en vigor la [Ley de Servicios Digitales](#) (DSA), un nuevo conjunto determinante de normas de la UE para un entorno en línea más seguro y responsable. La Ley de Servicios Digitales se aplica a todos los servicios digitales que conectan a los consumidores con bienes, servicios o contenidos. Crea nuevas y exhaustivas obligaciones para que las plataformas en línea reduzcan los daños y contrarresten los riesgos en línea, introduce una robusta protección de los derechos de los usuarios en línea y coloca a las plataformas digitales en un nuevo marco único de transparencia y responsabilidad. Diseñadas como un conjunto único y uniforme de normas de la UE, ofrecerán nuevas protecciones a los usuarios y seguridad jurídica a las empresas en todo el mercado único. La Ley de Servicios Digitales es una herramienta reguladora pionera a escala mundial y establece una referencia internacional para un enfoque regulador de los intermediarios en línea.

Nuevas responsabilidades para los servicios digitales

La Ley de Servicios Digitales introduce un nuevo conjunto exhaustivo de normas para los servicios de intermediación en línea sobre cómo deben diseñar sus servicios y procedimientos. Las nuevas normas incluyen nuevas responsabilidades para limitar la difusión de contenidos y productos ilícitos en línea, aumentar la protección de los menores y ofrecer a los usuarios más posibilidades de elección y mejor información. Las obligaciones de los diferentes agentes en línea se corresponden con su papel, tamaño e impacto en el ecosistema en línea. [Aquí](#) se ofrece una visión general de las mismas.

Todos los intermediarios en línea tendrán que cumplir/respetar/adecuarse a nuevas obligaciones de transparencia de amplio alcance para aumentar la rendición de cuentas y la supervisión, por ejemplo mediante un nuevo mecanismo de alerta para los contenidos ilícitos. Pero se introduce un régimen especial para las plataformas con más de 45 millones de usuarios: para las plataformas o motores de búsqueda de muy gran tamaño, se establecen obligaciones adicionales que incluyen evaluaciones anuales de amplio alcance de los riesgos de perjuicio de sus servicios en línea, por ejemplo en relación con la exposición a productos o contenidos ilícitos o la difusión de desinformación. En el marco de la Ley de Servicios Digitales, deberán establecerse medidas adecuadas de reducción de riesgos, y dichas plataformas y motores de búsqueda estarán sujetos a una auditoría independiente de sus servicios y de sus medidas de reducción de riesgos.

Las plataformas más pequeñas y las empresas emergentes se beneficiarán de un conjunto reducido de obligaciones, exenciones especiales de determinadas normas y un aumento fundamental de la claridad y la seguridad jurídicas para operar en todo el mercado único de la UE.

Refuerzo de las garantías de los derechos fundamentales en línea

Las nuevas normas protegen los derechos fundamentales de los usuarios en la UE también en el entorno en línea. Las nuevas protecciones de la libertad de expresión limitarán las decisiones arbitrarias de moderación de contenidos por parte de las plataformas y ofrecerán nuevas vías para que los usuarios actúen con conocimiento de causa contra la plataforma cuando se modere su contenido: por ejemplo, los usuarios de plataformas en línea tienen ahora medios para impugnar las decisiones de moderación de contenidos, incluso cuando estas decisiones se basen en las condiciones aplicadas por las plataformas. Los usuarios podrán presentar reclamaciones directamente a la plataforma, elegir un organismo de resolución extrajudicial de litigios o solicitar reparación ante los órganos jurisdiccionales.

Las nuevas normas también exigen que las condiciones de las plataformas se presenten de manera clara y concisa y que respeten los derechos fundamentales de los usuarios.

Además, las plataformas y los motores de búsqueda en línea de muy gran tamaño tendrán que llevar a cabo una evaluación exhaustiva de los riesgos para los derechos fundamentales, como, por ejemplo, la libertad de expresión, la protección de los datos personales y la libertad y el pluralismo

de los medios de comunicación en línea, así como los derechos del niño.

Nuevas competencias de supervisión de la Comisión

La Ley de Servicios Digitales crea un nivel sin precedentes de supervisión pública de las plataformas en línea en toda la Unión, tanto a escala nacional como de la UE. La Comisión tiene competencias para supervisar directamente las plataformas y los motores de búsqueda en línea de muy gran tamaño, que son empresas que llegan individualmente a más del 10 % de la población de la UE, es decir, aproximadamente 45 millones de personas. Además, cada Estado miembro tendrá que designar un coordinador de servicios digitales, que supervisará a otras entidades incluidas en el ámbito de aplicación de la Ley de Servicios Digitales, así como a las plataformas y motores de búsqueda en línea de muy gran tamaño para cuestiones no sistémicas. Los coordinadores nacionales y la Comisión Europea cooperarán a través de una Junta Europea de Servicios Digitales. Este mecanismo de cooperación a escala de la UE se establecerá entre los reguladores nacionales y la Comisión.

La Comisión está creando un [Centro europeo para la transparencia algorítmica](#) (CETA) para apoyar su función supervisora con conocimientos multidisciplinares internos y externos. El Centro prestará apoyo con evaluaciones para determinar si el funcionamiento de los sistemas algorítmicos está en consonancia con las obligaciones de gestión de riesgos que establece la Ley de Servicios Digitales para las plataformas y los motores de búsqueda en línea de muy gran tamaño a fin de garantizar un entorno en línea seguro, predecible y fiable.

Próximos pasos

Tras la entrada en vigor de la Ley de Servicios Digitales hoy, las plataformas en línea dispondrán de tres meses para comunicar el número de usuarios finales activos (17 de febrero de 2023) en sus sitios web. La Comisión también invita a todas las plataformas en línea a que le notifiquen los números publicados. Sobre la base de estos números de usuario, la Comisión evaluará si una plataforma debe ser designada como plataforma o motor de búsqueda en línea de muy gran tamaño. Una vez tomada la decisión de designación por parte de la Comisión, la entidad en cuestión dispondrá de cuatro meses para cumplir las obligaciones derivadas de la Ley de Servicios Digitales, incluida la realización del primer ejercicio anual de evaluación de riesgos y su comunicación a la Comisión. Los Estados miembros de la UE tendrán que facultar a sus coordinadores de servicios digitales a más tardar el 17 de febrero de 2024, fecha general de entrada en vigor de la Ley de Servicios Digitales, cuando esta será plenamente aplicable a todas las entidades incluidas en su ámbito de aplicación.

Contexto

El 15 de diciembre de 2020, la Comisión presentó la [propuesta](#) sobre la Ley de Servicios Digitales junto con la propuesta sobre la Ley de Mercados Digitales como marco global para garantizar un espacio digital más seguro y justo para todos. La Ley de Mercados Digitales [entró en vigor](#) el 1 de noviembre de 2022.

Los servicios digitales incluyen una amplia categoría de servicios en línea, desde simples sitios web hasta servicios de infraestructuras de internet y plataformas en línea. Las normas especificadas en la Ley de Servicios Digitales se refieren principalmente a los intermediarios y las plataformas en línea. Por ejemplo, los mercados en línea, las redes sociales, las plataformas de intercambio de contenidos, las tiendas de aplicaciones y las plataformas de viajes y alojamiento en línea.

Más información

[Texto del Diario Oficial de la UE](#)

[Ley de Servicios Digitales: preguntas y respuestas](#)

[Ley de Servicios Digitales: página informativa](#)

[Paquete de la Ley de Servicios Digitales](#)

IP/22/6906

Members of the college said:

Con la Ley de Servicios Digitales, disponemos ahora de una legislación clara. Las plataformas en línea constituyen el núcleo de algunos de los aspectos clave de nuestra vida cotidiana, nuestras democracias y nuestras economías. Es lógico garantizar que estén a la altura de sus responsabilidades a la hora de reducir la cantidad de contenidos ilícitos en línea y limitar otros perjuicios en línea, así como de proteger los derechos fundamentales y la seguridad de los usuarios.

La Comisión se prepara rápidamente para asumir su nuevo papel de supervisor de algunas de las empresas tecnológicas más grandes e influyentes del mundo, que millones de ciudadanos y empresas europeas utilizan cada día. Estas nuevas normas marcan el comienzo de una nueva era, en la que las grandes plataformas en línea ya no se comportarán como si fueran demasiado grandes como para tener que preocuparse. El nuevo código normativo se verá respaldado por una estricta supervisión y ejecución, con multas de hasta el 6 % del volumen de negocios mundial en caso de incumplimiento e incluso la prohibición de operar en el mercado único de la UE en caso de reiteradas infracciones graves. Todos pueden hacer negocios en la UE siempre que cumplan estas nuevas normas.

Personas de contacto para la prensa:

[Johannes BÄHRKE](#) (+32 2 295 86 15)

[Charles MANOURY](#) (+32 2 291 33 91)

Solicitudes del público en general: [Europe Direct](#) por teléfono [00 800 67 89 10 11](#) , o por [e-mail](#)

Related media

 [Illustrations on disinformation](#)

ANEXO N.º 05: MEDIDAS CONTRA LA RADICALIZACIÓN FINANCIADAS POR LA UE.

Ejemplos de medidas contra la radicalización financiadas por la UE

Medida	Objetivo para hacer frente a la radicalización	Financiación	Gestión
Red para la Sensibilización frente a la Radicalización (RSR)	Prestar apoyo a los Estados miembros en el diseño y la implementación del trabajo de prevención efectivo, proporcionando directrices y manuales para el establecimiento de estructuras multiinstitucionales y la creación de una plataforma para el intercambio de experiencias y prácticas, y realizando nuevos inventarios de la investigación sobre la radicalización.	Fondo de Seguridad Interior-Policía	DG Migración y Asuntos de Interior
Subvenciones a la investigación	Tender puentes entre los académicos y los profesionales de la seguridad en el ámbito de la radicalización para reforzar la capacidad de los Estados miembros para afinar los enfoques políticos existentes y desarrollar nuevas políticas y prácticas (Temas de investigación: desarrollar un enfoque integral sobre la radicalización violenta y tendencias de radicalización contemporáneas)	Programa Horizonte 2020	DG Migración y Asuntos de Interior DG Investigación e Innovación
Proyectos de seguridad en gestión directa y compartida	Desarrollar instrumentos de divulgación, compromiso y asistencia a agentes locales y familias para prevenir la radicalización	Fondo de Seguridad Interior-Policía	DG Migración y Asuntos de Interior

Contrarrestar la propaganda terrorista

Medida	Objetivo para hacer frente a la radicalización	Financiación	Gestión
Unidad de Notificación de Contenidos de Internet de la UE (UNCI)	Contrarrestar la propaganda terrorista en línea	Europol	Europol
Foro de la UE sobre Internet	Iniciativa de la Comisión para involucrar a las empresas de Internet en la lucha contra la propagan	Fondo de Seguridad Interior	DG Migración y Asuntos de Interior
Red Europea de Comunicaciones Estratégicas	Dotar a los Estados miembros, la sociedad civil y las instituciones de la UE de especialización para desarrollar marcos políticos, campañas de comunicación o iniciativas individuales. Proporcionar una red para compartir e intercambiar las mejores prácticas y apoyo práctico y asesoramiento para ayudar a desarrollar contranarrativas eficaces.	Fondo de Seguridad Interior	DG Migración y Asuntos de Interior
Proyectos de seguridad en gestión directa y compartida	Abordar el problema de contenido en línea que pueda conducir a radicalización	Fondo de Seguridad Interior-Policía	DG Migración y Asuntos de Interior

Promover sociedades inclusivas y resistentes

Medida	Objetivo para hacer frente a la radicalización	Financiación	Gestión
Asociaciones transnacionales	Desarrollar enfoques de política innovadores y prácticas que prioricen la inclusión social, el fomento de valores comunes y el entendimiento intercultural	Erasmus+	DG Educación, Juventud, Deporte y Cultura
Apoyo a la reforma de la política	Difundir y extender buenas prácticas innovadoras que se inscriben en el ámbito de la Declaración de París		
Servicio Voluntario Europeo	Promover valores fundamentales y llegar a las personas y comunidades desfavorecidas		
Trabajadores jóvenes	Desarrollar un conjunto de herramientas de mejores prácticas sobre cómo: - ayudar a los jóvenes a aumentar su resiliencia democrática, adquirir conocimientos mediáticos y desarrollar un espíritu crítico; - enseñar a los jóvenes a resolver conflictos y respetar las opiniones de los demás; - detectar riesgos de marginación o identificar grupos vulnerables		
eTwinning	Conectar a profesores y aulas de toda Europa a través de la plataforma de Internet eTwinning para determinar las mejores prácticas a la hora de abordar la diversidad en el aula y transmitir valores comunes a los alumnos y detectar riesgos de marginación o identificar grupos vulnerables	Fondo Social Europeo	DG Empleo, Asuntos Sociales e Inclusión DG Política Regional y Urbana
Apoyar planes nacionales y pequeños proyectos locales	Fomentar la inclusión social de los grupos desfavorecidos, por ejemplo a través de programas de formación y planes de apoyo social a medida Ayudar a las escuelas a abordar la cuestión del abandono escolar temprano y aumentar el acceso a una educación de calidad para todos		
Proyectos de empleo e innovación social	Financiar proyectos innovadores sobre el terreno que fomenten la inclusión social		
Proyectos sobre derechos, igualdad y ciudadanía	Mejorar el entendimiento entre las comunidades, incluidas las religiosas, para prevenir y combatir el racismo y la xenofobia por medio de actividades interreligiosas e interculturales	Programa «Derechos, Igualdad y Ciudadanía»	DG Justicia y Consumidores
Proyectos de seguridad en gestión directa y compartida	Sensibilizar y formar a los profesionales que trabajan en primera línea para que reconozcan y respondan al proceso de radicalización de combatientes extranjeros potenciales	Fondo de Seguridad Interior-Policía	DG Migración y Asuntos de Interior

Identificar y tratar a personas radicalizadas

Medida	Objetivo para hacer frente a la radicalización	Financiación	Gestión
Programas de rehabilitación y desradicalización	Rehabilitación y desradicalización dentro y fuera de los centros penitenciarios, herramientas de evaluación de riesgos y formación de profesionales	Programa «Justicia»	DG Justicia y Consumidores
Formación de personal penitenciario y de libertad vigilada	Hacer partícipes a la Confederación Europea de la Libertad Vigilada y la Organización Europea de Prisiones y Servicios Correccionales en formación específica para personal penitenciario y de libertad vigilada		

Hacer frente a la radicalización en países fuera de Europa

Medida	Objetivo para hacer frente a la radicalización	Financiación	Gestión
Medidas de lucha contra el terrorismo	Prestar apoyo específico contra el terrorismo a terceros países	Fondo Europeo de Desarrollo e Instrumento en pro de la estabilidad y la paz	DG Cooperación Internacional y Desarrollo
		Instrumento Europeo de Vecindad	DG Política de Vecindad y Negociaciones de Ampliación
Incorporación de la dimensión de lucha contra la radicalización	Incorporar las cuestiones de lucha contra la radicalización en varios tipos de apoyo a terceros países	Fondo Europeo de Desarrollo e Instrumento en pro de la estabilidad y la paz	DG Cooperación Internacional y Desarrollo
		Instrumento Europeo de Vecindad	DG Política de Vecindad y Negociaciones de Ampliación
eTwinning Plus	Ampliar la plataforma eTwinning a determinados países de la vecindad europea, en particular a los que afrontan problemas relacionados con la radicalización violenta y en los que el diálogo intercultural es más necesario	Erasmus+	DG Educación, Juventud, Deporte y Cultura

Fuente: TCE a partir de la Comunicación de la Comisión titulada «Apoyo a la prevención de la radicalización que conduce al extremismo violento».

