TESIS DOCTORAL

2018

CIBERTERRORISMO: AMENAZA A LA SEGURIDAD. RESPUESTA OPERATIVA Y LEGISLATIVA, NACIONAL E INTERNACIONAL

AUTOR: VICENTE PONS GAMÓN

PROGRAMA DE DOCTORADO EN DERECHO Y CIENCIAS SOCIALES

DIRECTOR: Dr. D. FERNANDO MOURE COLÓN
CODIRECTORA: Dra. Dña. MARÍA TERESA MARCOS MARTÍN

TESIS DOCTORAL

2018

CIBERTERRORISMO: AMENAZA A LA SEGURIDAD. RESPUESTA OPERATIVA Y LEGISLATIVA, NACIONAL E INTERNACIONAL

Autor:

VICENTE PONS GAMÓN
Licenciado en Ciencias Empresariales
Postgrado en Seguridad

Director
Dr. D. FERNANDO MOURE COLÓN
Centro Universitario de la Guardia Civil

Codirectora
Dra. Dña. MARÍA TERESA MARCOS MARTÍN
Universidad Nacional de Educación a Distancia

AGRADECIMIENTOS

“A mi familia, muy especialmente a mi madre y a mi padre, por apoyarme todos los días desde que nací, por estar siempre ahí, a mi lado, pendientes de mi y pensando en hacerme fácil lo que yo veo difícil. A mi sobrina por alegrarme el dia, cada vez que la veo.

A todos mis amigos por dejar de verme en mucho tiempo, permitiéndome que desapareciera de la vida social y sin embargo, estar al otro lado del teléfono siempre dándome fuerzas y animándome.

Al Profesor Fontes por mi estancia en Portugal que nunca olvidaré.

Y de forma muy especial, al Dr. Rafael Benavent por su participación y empuje, a mi directora la Dra. Mª Teresa Marcos por toda su aportación y a mi director de tesis el Coronel Dr. Fernando Moure, sin él no hubiera sido posible mi proyecto, por estar apoyándome contínuamente y dirigir la tesis como si fuera la suya propia.
Gracias, Rafa.
Gracias, Teresa.
Gracias, Fernando.

Al Señor por darme fuerzas todos los días, cuando me levanto, empujándome hacia adelante y por darme todo lo que tengo, que me hace disfrutar de mi trabajo”.

GRACIAS A TODOS.

ÍNDICE

TABLA DE ILUSTRACIONES

ABREVIATURAS

AED.-	Agencia Europea de Defensa.
AIVD.-	Servicio holandés de Seguridad e Información.
ANS.-	Autoridad Nacional de Seguridad (Portugal).
AMIA.-	Asociación Mutual Israelita Argentina. Sufrió atentado terrorista con coche bomba el 18/07/1994.
AndaluciaCERT.-	Centro de respuesta a incidentes de ciberseguridad de Andalucía.
ANSSI.	Agencia Nacional de Ciberseguridad de Francia.
ASEAN.-	Asociación de Naciones del Sudeste Asiático (Association of Southeast Asian Nations).
AUGC.-	Asociación Unificada de Guardias Civiles.
BIT.-	Brigada de Investigación Tecnológica de la Policía Nacional.
BM.-	Banco Mundial.
CAP.-	Centro de Análisis y Prospectiva de la Guardia Civil.
CATA.-	Centro de Alerta Temprana Antivirus.
CCD COE.-	Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN.
CCN.-	Centro Criptológico Nacional.
CCN-CERT.-	Equipo de respuesta a emergencias cibernéticas del CCN (Centro Criptológico Nacional).
CDM.-	Concepto de Ciberdefensa Militar.
CDMA.-	Autoridad para la gestión en ciberdefensa de la OTAN.
CDMB.-	Consejo para la gestión en ciberdefensa de la OTAN.
CDN.-	Convención sobre Derechos del Niño.
CEPOL.-	Agencia de la UE que promueve la cooperación policial europea e internacional a través de la formación.
CERT´s.-	*Computer Emergency Response Team*.
CERT-EU.-	Equipo de Respuesta ante Incidentes de la Unión Europea.
CERTSI.-	CERT de Seguridad e Industria.
CESICAT.-	Centro de Seguridad de la Información de la Generalitat de Catalunya.
CIS.-	Centro de Información de Seguridad.

CISP.-	Asociación de Intercambio sobre Seguridad Cibernética (UK).
CITCO.-	Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado.
CIWIN.-	Red de alerta en relación con infraestructuras críticas.
CNC.-	Consejo Nacional de Ciberseguridad.
CNCS.-	Centro Nacional de Ciberseguridad (Portugal).
CNI.-	Centro Nacional de Inteligencia (Ministerio de Presidencia).
CNPIC.-	Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
COSDEF.-	Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa.
CP.-	Código Penal.
CPA.-	*Commercial Product Assurance*. Garantía de productos comerciales. (Reino Unido).
CSCE.-	Conferencia sobre la Seguridad y la Cooperación en Europa.
CSIRT.-	Red de equipos de respuesta a incidentes de seguridad informática (UE).
CSIRT-CV.-	Centro de Seguridad TIC de la Comunitat Valenciana.
CSN.	Consejo de Seguridad Nacional.
CSPN.-	*Certification de Sécurité de Premier Niveau* (Francia).
CUGC.-	Centro Universitario de la Guardia Civil.
DAESH.-	Es el acrónimo árabe del ISIS (en inglés, Estado Islámico de Irak y Siria).
DDoS.-	*Distributed Denial of Service* (ataque distribuido de denegación de servicio).
DGST.-	Dirección General de Supervisión del Territorio (Marruecos).
DHDS.-	*Djama Houumat Edaawa Essalafia* (Grupo de Partidarios de la Corriente Salafista).
DIRPC.-	Dispositivo integrado de respuesta política de la UE a las crisis.
DNIe.-	Documento Nacional de Identidad (DNI) electrónico.
DNS.-	*Domine name server* (nombre del servidor del dominio).
DPPC.-	Comité de Planeamiento y Política de Defensa (*Defence Policy and Planning Committee*).
EAPAC.-	*European Partnership Council* (Consejo de la Asociación Europea).
EC3.-	Centro Europeo de Cibercrimen.
ECTC.-	Centro Europeo Contra el Terrorismo.
EDITE.-	Equipos de Investigación Tecnológica de la Guardia Civil.
EI.-	Estado Islámico.
EIN.-	Estrategia de Información Nacional (Portugal).
EMAD.-	Estado Mayor de la Defensa.
EMGFA.-	Estado Mayor General de las Fuerzas Armadas (Portugal).
EMI.-	*Electro Magnetic Interference.*
EMP.-	Pulso electro magnético.
ENISA.-	Agencia Europea de Seguridad de las Redes y de la Información

	(*Agency for network and information security*).
ENS.-	Esquema Nacional de Seguridad.
ENSD.-	Estrategia de Seguridad y Defensa del Estado (Portugal).
ENSI.-	Estrategia de Seguridad Nacional de la Información (Portugal).
EPRS.-	Servicio de Investigación Parlamentaria Europea.
ESN.-	Estrategia de Seguridad Nacional.
ETA.-	*Euskadi Ta Askatasuna* (País Vasco y libertad).
EUROPOL.-	Agencia de la Unión Europea para la Cooperación Policial.
EUROSTAT.-	Oficina de Estadística de la Unión Europea.
FATF.-	*Financial Action Task Force* (Grupo de acción financiera internacional).
FBI.-	*Federal Bureau of Investigation*.
FCSE.-	Fuerzas y Cuerpos de Seguridad del Estado.
FDJP.-	*Federal Department of Justice and Police*.
FMI.-	Fondo Monetario Internacional.
FSI.-	Fondo de Seguridad Interior.
FVEY.-	*Five Eyes*. Alianza de inteligencia de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos.
G-8.-	Grupo de los 8 países más industrializados del mundo (Rusia, Canadá, Estados Unidos, Francia, Italia, Alemania, Reino Unido y Japón).
GAFI.-	Grupo de Acción Financiera Internacional.
GAFISUD.-	Grupo de Acción Financiera de Sudamérica.
GCT.-	Grupo de Ciberterrorismo de la Guardia Civil.
GDT.-	Grupo de delitos telemáticos de la Guardia Civil.
GECENI.-	Grupo de Estudio sobre las Contribuciones a una Estrategia Nacional de Información del Instituto de Defensa Nacional (Portugal).
GICM.-	Grupo Islámico Combatiente Marroquí.
GNR.-	Guardia Nacional Republicana (Portugal).
GRAPO.-	Grupos de Resistencia Antifascista Primero de Octubre.
HEMP.-	Pulso electromagnético de gran altitud.
I+D+i.-	Investigación + Desarrollo + innovación.
ICI.-	*Istanbul Cooperation Iniciative* (Iniciativa de Cooperación de Estambul).
ICT.-	*Information Communications Tecnology*.
INCIBE.-	Instituto Nacional de Ciberseguridad.
INS.-	Instituto Nacional de Salud.
INTCEN.-	*Intelligent Centre* (Centro de inteligencia de la Unión Europea).
INTECO.-	Instituto Nacional de Tecnologías de la Comunicación.
IPCR.-	*Integrated Political Crisis Response*. Respuesta política integrada frente a crisis.
IRC.-	*Internet Relay Chat*.
IRU.-	Unidad de Referencia de Internet.

IS.-	*Islamic State*. Estado Islámico.
ISIL.-	*Islamic State of Iraq and the Levant* (Estado Islámico de Irak y Levante). "ISIS", "*Daish*", "*Daesh*", "*Islamic State group*".
JEMAD.-	Jefe del Estado Mayor de la Defensa.
MCCD.-	Mando Conjunto de Ciberdefensa.
MDE.-	Es un acuerdo o convenio.
MICE.-	*Money, Ideology, Compromise & Ego* (Dinero, Ideología, Compromiso y Autorrealización personal).
MoU.-	*Memorandum of understanding* (Memorando de Entendimiento
MUD.-	Mercado Único Digital.
NC3.-	Comité de Consulta, Mando y Control (*NATO Consultation, Command and Control - C3*).
NC3A.-	Agencia de Consulta, Mando y Control (*NATO C3 Agency*).
NCIA.-	*NATO Communications and Information Agency*.
NCIRC.-	*Computer Incident Response Capability* (capacidad de respuesta de la OTAN a incidentes informáticos).
NCSA	Agencia de servicios de Información y Comunicación (*NATO Communication and Information Systems Services Agency*)
NeoGend.-	*Nouvel équipement opérationnel Gendarmerie Nationale* (Francia), nuevo equipo operacional de la Gendarmería Nacional francesa.
NFS.-	Protección de servicios de red.
NICP.-	*NATO Industry Cyber Partnership*.
NIS.-	Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. (*Network and information Systems*).
NMA	Autoridad Militar (*NATO Military Authority*).
NNUU.-	Naciones Unidas.
NSA.-	*National Security Agency*.
OCC.-	Oficina de Coordinación Cibernética (Ministerio de Interior).
OCDE.-	Organización de Cooperación y Desarrollo Económico.
ODINO.-	*Operational Device for Information Networking, and Observation* (Dispositivo operativo para redes de información y observación).
OEDT.	Observatorio Europeo de Drogas y Toxicomanías.
OIEA.-	Organismo Internacional de Energía Atómica.
ONS.-	Oficina Nacional de Seguridad.
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.
PEPIC.-	Programa Europeo para la Protección de las Infraestructuras Críticas.
PESCO.-	Permanent structured cooperation (cooperación estructurada permanente).
PGDL.-	*Procuradoría-Geral Distrital de Lisboa*.

PKK	Partido de los Trabajadores de Kurdistán (en kurdo, *Partiya Karkerên Kurdistan*, PKK; en turco, *Kürdistan İşçi Partisi*). Su brazo armado se denomina Fuerzas de Defensa Popular (HPG).
PP.-	Partido Popular.
PSOE.-	Partido Socialista Obrero Español.
PSP.-	Policía de Seguridad Pública (Portugal).
PYMES.-	Pequeñas y medianas empresas.
REDIRIS.-	Red Española para la Interconexión de Recursos informáticos
RFI.-	*Radio Frequency Interference*.
SAN.-	Sentencia de la Audiencia Nacional.
SCADA.-	Guías de interés para la seguridad de los sistemas de control industrial (CNPIC y CCN).
SDGTIC.-	Subdirección General Tecnologías de la Información y Comunicación del Ministerio de Defensa.
SEGINFOPER.	Seguridad de la Información de las Personas
SEPBLAC.-	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias de España.
SESIAD.-	Secretaría de Estado para la Sociedad de la Información y Agenda Digital.
SIGINT.-	Inteligencia de señales (*Signals Intelligence*).
SOG-IS.-	*Senior Officials Group Information System Security*. Sistema de Seguridad de la información de los altos funcionarios.
SPIIN.-	Sistema Nacional de Protección de Infraestructura de Información (Portugal).
SSI.-	Sistema de Seguridad Interior (Portugal).
STC	Sentencia Tribunal Constitucional.
STS	Sentencia Tribunal Supremo.
SUP.-	Sindicato Unificado de la Policía.
TAK.-	"Halcones de la Libertad del Kurdistán", grupo armado escindido del PKK.
TATP.-	Triperóxido de Triacetona. Explosivo "casero" que utiliza el Estado Islámico.
TEDAX.-	Técnico Especialista en Desactivación de Artefactos Explosivos.
TEDH	Tribunal Europeo de Derechos Humanos.
TIC.-	Tecnologías de la Información y las Comunicaciones.
TPIM.-	*Terrorism Prevention and Investigation Measures*. Medidas de Investigación y Prevención del Terrorismo (Reino Unido 2011).
TUE.-	Tratado de Maastricht sobre la Unión Europea.
UCAT.-	Unidad de Cooperación Antiterrorismo (Portugal).
UCO.-	Unidad Central Operativa de la Guardia Civil.
UCS.-	Unidad de Ciberseguridad de la Guardia Civil.
UE.-	Unión Europea.
UIF.-	Unidad de inteligencia financiera.
UIT.-	Unión Internacional de las Telecomunicaciones.

UKUSA.-	Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda.
USA.-	*United States of America* / Estados Unidos de America)
UTPJ.-	Unidad Operativa de Inteligencia Criminal de la Guardia Civil.
11-M.-	Atentado terrorista yihadista de Madrid 11 de marzo de 2004.
11-S.-	Atentado terrorista de Al Qaeda en Estados Unidos 11 de septiembre de 2001.

INTRODUCCIÓN

Esta investigación surge como respuesta ante los grandes cambios acontecidos en el escenario mundial a raíz del desarrollo y expansión de las tecnologías de la comunicación.

Estos cambios han desarrollado y potenciado los estándares del bienestar, facilitando la vida a los seres humanos en muchos sentidos y favoreciendo e impulsando grandes avances en todas las áreas: medicina, comunicación, tecnología, etc. En sentido opuesto se han implementado también facilidades y capacidades destructivas, que puestas en manos de los delincuentes han supuesto la aparición de infinidad de actos y situaciones delictivas nunca vistas ni imaginadas con anterioridad.

En la primera parte de la investigación, nuestro objetivo es realizar un estudio de las características más importantes de este fenómeno delictivo, de forma que al leer el trabajo tengamos una idea clara y extensa de éste y cuál es su repercusión socialmente a nivel mundial.

En la segunda parte, estudiaremos la reacción de las naciones en la dirección de poder controlar el ciberespacio y combatir todos los delitos que se produzcan, siempre desde la legalidad y el respeto de los derechos humanos, base fundamental de convivencia de las naciones civilizadas.

Siguiendo esta línea de investigación, profundizaremos en el caso concreto del estado español y las recientes actualizaciones realizadas en su legislación y concretamente sus leyes propiamente referidas al terrorismo y ciberterrorismo, en su moderna especialización, siempre desde el marco de la Unión Europea, que es

la que marca las nuevas directrices para legislar este fenómeno, buscando el camino de la estandarización legislativa en materia de terrorismo dentro de sus amplias fronteras y en cada uno de sus estados. Analizaremos casos concretos en sentencias y presentaremos estas leyes, su aplicación y resultados.

Una vez realizada la labor de determinar, clasificar los nuevos delitos y conocer las leyes que deben regularlos, podremos hablar de las estrategias, que tanto España como nación, la Unión Europea y organizaciones como la OTAN, toman como directrices en sus actuaciones, para poder combatir los efectos del nuevo espacio delictivo y a sus protagonistas, los delincuentes y sus acciones que están alterando la convivencia pacífica y el respeto a la ley en las naciones occidentales.

Para finalizar, completaremos este estudio con un trabajo de campo sobre el área jurídica en España y más concretamente sobre los objetos delictivos del ciberterrorismo y las nuevas modificaciones en leyes de esta materia; realizando unas encuestas al respecto, entre los grupos que intervienen en este proceso legal de determinación de los delitos, aplicación de las leyes y operatividad para poder implementar éstas en la sociedad. Son encuestas realizadas a Jueces, abogados y FCSE (Fuerzas y Cuerpos de Seguridad del Estado), lo que nos permitirá ver los resultados obtenidos tras las modificaciones en la ley en su sentido más práctico.

Objetivo

Como principal objetivo, este trabajo trata de dar una visión teórico-práctica concreta del fenómeno del ciberterrorismo y de su jurisprudencia actual en el Estado español, brindando un aporte significativo a los estudios de los delitos penales; así como describir la política antiterrorista en el estado español y el grado de éxito en su aplicación, pero sobre todo analizar la incidencia y aplicación práctica de la legislación Penal en materia de terrorismo.

Desde un punto de vista teórico analizar en el estado español y la UE la situación actual del terrorismo, normativa y su entramado defensivo.

Desde un punto de vista práctico ver la incidencia y aplicación de la legislación Penal en materia de terrorismo, a partir y antes de su modificación en el 2015, sobre actos y actuaciones terroristas cometidas en el estado español.

Objetivos específicos

- Describir el marco jurisprudencial de la política antiterrorista en el estado español y el grado de éxito en su aplicación.
- Evidenciar la necesidad que tienen los estados de standarizar sus leyes en esta materia, siguiendo las líneas de la UE.
- Identificar el contexto actual del terrorismo y ciberterrorismo en el estado español y la UE.
- Caracterizar el comportamiento del terrorismo y ciberterrorismo en el estado español dentro del marco de la UE.

Hipótesis

- Los cuerpos de seguridad antiterrorista han conseguido evidentemente y en contra de su crecimiento exponencial, un impacto en la disminución de esos ataques, pero este no ha sido suficiente debido a la complejidad del delito.
- Debido a la estrategia geoespacial que presenta el ciberterrorismo, es necesario el desarrollo y continúa mejora la de los mecanismos legales transnacionales donde cooperan multilateralmente todos los países afectados.
- La Unión Europea se ha movilizado en sus ámbitos policiales y legislativos para buscar la operatividad contra el terrorismo dentro de sus fronteras y de esta forma conseguir que sus ciudadanos estén más seguros en ellas.
- El sistema defensivo en la UE y sus estados, a su vez interconectados con la OTAN es tan grande y complejo que lo podíamos denominar ENTRAMADO DEFENSIVO.
- Este medio es tan cambiante y complejo, que las estrategias de defensa y sus métodos de actuación necesitan de una contante supervisión y actualización.

- El éxito para combatir el ciberdelito se basa en la tecnología, factor humano y sobre todo en la cooperación internacional de todos los estados y sus fuerzas de seguridad.

Metodología

Analizar las normativas de seguridad y leyes actuales del código penal en materia de terrorismo y ciberterrorismo, requiere estrategias que permitan la comprensión de la incidencia de la legislación de Seguridad Nacional frente al terrorismo en el estado español, en la medida que ésta se contrasta a la luz de leyes anteriores, donde la metodología que se propone para este fin, intenta responder a necesidades investigativas relacionadas a la jurisprudencia constitucional del Tribunal Supremo, cuyo análisis se centrará en su aplicabilidad.

La presente investigación se sustenta en el enfoque cualitativo, "el cual permite hacer una aproximación global a las situaciones sociales para explorarlas, describirlas y comprenderlas" (Bonilla y Rodríguez, 1997), haciendo lectura crítica sobre las actuaciones judiciales aplicadas y creadas en las sentencias de constitucionalidad, a través de la descripción de las mismas, lo que permitirá la comprensión del estado actual de la ley y su incidencia en los contextos sociales en los cuales se aplica; desde una perspectiva hermenéutica, a partir de la cual se privilegia los discursos y significados de los actores, es holística porque comprende la realidad jurídica desde diversos puntos de vista; es de naturaleza inductiva porque no pretende formular leyes universales, sino más bien entiende la complejidad de un específico contexto jurídico, aplicado a un contexto también especifico, es heurística y generativa, donde las hipótesis, teorías y normativas en seguridad dentro del estado español y la UE son tomadas como guías en el proceso de conocimiento y se van modificando y retroalimentando de acuerdo a las circunstancias, dada la constante actualización del enfoque.

Con la metodología cualitativa se busca ante todo entender el contexto jurídico y normativo desde la posición epistemológica del constructivismo, y la complejidad; con la perspectiva investigador(a), y el investigado(a) en una relación de construcción de conocimiento (Torres, citado por Ballén, et.al., 2007), desde lo que recoge, describe e interpretan los procesos sociales. Se hará uso además de

algunas herramientas cuantitativas para alimentar el proceso de análisis, en la medida que toda cantidad es el reflejo numérico de una cualidad (Ander egg).

El enfoque elegido para llevar a cabo esta investigación es el Descriptivo y Analítico, donde los actores darán cuenta de las de las propiedades contenidas en la regla jurisprudencial dentro del contexto jurídico español. **En cuanto al método de estudio**, se hará mediante la interpretación y descripción detallada de (7) sentencias, además del análisis de la Legislación en materia Antiterrorista de mediados del 2015 y presente año en comparación con los años 2014 y principios del 2015, para contrastar su incidencia en dicho contexto, se propone además la realización de entrevistas semiestructuradas a 10 Jueces, 20 abogados y 125 mandos de las fuerzas de seguridad de diversos países. El criterio de selección, de las y los entrevistados responde exclusivamente a su pertenencia al ámbito de la abogacía, adjudicatura y seguridad.

El periodo de inflexión escogido va desde la modificación de la ley en 2015 y se tendrá en cuenta como unidades de análisis, la jurisprudencia de la ley, las sentencias llevadas a cabo, incidencia en la política antiterrorista y la manera como opera el ciberterrorismo en el estado español.

Adquisición de datos

En las revisiones documentales acerca del ciberterrorismo, ha sido complejo encontrar estudios científicos sobre el mismo. Sin embargo, algunas tesis mexicanas abordan el tema desde el caso español, lo que nos permite hacer un análisis desde una perspectiva internacional.

Un trabajo, desarrollado por IGNACIO JOSÉ SUBIJANA ZUNZUNEGUI titulado *"El ciberterrorismo: una perspectiva legal y judicial"* plantea que la globalización conlleva la implantación de un modelo social pergeñado en torno, entre otros, a los valores de ubicuidad, virtualidad y celeridad, lo que en el orden penal conlleva a la necesidad de afrontar fenómenos delictivos protagonizados por organizaciones criminales de carácter transnacional que hacen un uso perverso de las tecnologías de la información y la comunicación (SUBIJANA, 2008, p.167).

Esto nos permitirá entender, la importancia del contexto en el que se desarrolla el terrorismo, los componentes que los dirigen permiten que se desarrollen de forma estructural, para su posible actuación.

Además, presenta una revisión de las propuestas normativas a través de la aproximación de las legislaciones y la cooperación policial y judicial en y entre los Estados, las cuales intentan garantizar una adecuada respuesta pública a la problemática del ciberterrorismo, superando la indiscutible insuficiencia de un tratamiento territorial de esta específica criminalidad (SUBIJANA, 2008, p.167).

Se ha modificado en el 2015 la directiva europea relativa el blanqueo de capitales o la financiación del terrorismo “Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) nº 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión”. (Publicado: «DOUE» núm. 141, de 5 de junio de 2015, páginas 73 a 117, Departamento: Unión Europea, Referencia: DOUE-L-2015-81123), intentamos ver y analizar las últimas actualizaciones de normativa europea en esta materia.

Ahora mismo la directiva europea contra el terrorismo incluye el castigo a los que "ayuden" o sean cómplices en la comisión de delitos terroristas sin concretar que éstos tengan la intención de ayudar.

“La Comisión de Libertades Civiles de la Unión Europea, dentro del texto de las Directivas Europeas contra el Terrorismo, han desarrollado una normativa para contrarrestar el efecto destructivo de este”.

Nos encontramos ante una gran controversia: hasta dónde puede llegar nuestro derecho a la intimidad como ciudadanos europeos, cuando este se cruza con investigaciones y actuaciones tanto policiales como judiciales sobre ciudadanos residentes en Europa “ X-net denuncia : Directiva contra el Terrorismo: El Parlamento Europeo contra nuestras libertades” (Xnet, 2016, *https://xnet-x.net/directiva-**terrorismo**-recorte-libertades).*

Se *analiza los elementos esenciales de la actual estrategia de seguridad nacional, y su comparativa con su predecesora de 2013 y con las estrategias de seguridad nacional de nuestro entorno, también nos centramos en concreto en las estrategias de ciberseguridad española y de su entorno.*

El trabajo esboza que, en el ámbito de la Defensa, la Directiva de Defensa Nacional del año 2004 comenzó a contemplar una concepción más amplia de los riesgos y amenazas que presentaba la seguridad, llegando en el 2008 a resaltar la aparición de nuevos riesgos y amenazas para la paz, estabilidad y seguridad internacional, como era el caso del terrorismo transnacional. Estos cambios legislativos, permiten observar la estrategia estatal frene a la legislación, en el manejo del problema del ciberterrorismo (García, 2014, p. 51).

Establece, que este delito tiene un alcance global y que constituye, junto al crimen organizado, la amenaza más grave para la seguridad por el peligro que podía suponer el que grupos terroristas pudiesen apropiarse de armas de destrucción masiva (Ibídem).

Este estudio brinda herramientas de análisis crítico frente al ciberterrorismo, proponiendo la necesidad de extender lazos internos e internacionales para contrarrestar esas prácticas, que son de gran riesgo para el desarrollo de nuestras naciones.

Mónica Olvera Gorts, presenta un trabajo titulado *"Ciberterrorismo e infraestructuras críticas"***,** contempla el ciberterrorismo como formas de agresión a la sociedad derivadas del mal uso de las tecnologías de la información la comunicación (TIC) (Olvera, 2013, p. 1).

Así mismo se muestran diversas acciones emprendidas por España y otros estados en materia de ciber-seguridad," Estrategia española de Ciberseguridad" y "Estrategia Portuguesa de Ciberseguridad".

Un apartado desde mi punto de vista de gran interés es el análisis de casos específicos que han tenido lugar en España, donde ponemos analizar los procesos acontecidos (delito - actuación policial- actuación judicial - jurisprudencia) siendo de gran relevancia el estudio de la jurisprudencia.

Con esa revisión de antecedentes, presentamos la necesidad de seguir avanzando en los estudios del terrorismo, como una forma de generar hallazgos significativos que posibiliten la creación de estrategias de seguridad pertinentes, para mejorar el tratamiento que se la da al delito con una jurisprudencia, a fin que permita la disminución de esos actos delictivos.

Descripción de contenido

Este trabajo tratará de desarrollar un análisis de la jurisprudencia actual en la comunidad española, brindando un aporte significativo a los estudios de los delitos penales.

Además, analizará estrategias aspectos específicos de defensa contra el ciberterrorismo y el terrorismo en general, brindará la posibilidad de manejar la información actualizada, que podrá ser consultada como documento de apoyo en los estudios de ciberseguridad y ciberdelitos.

Por otro lado, permitirá un análisis cronológico de la jurisprudencia, sus cambios en las últimas modificaciones legales, mostrando el impacto del mismo en el tratamiento del terrorismo.

Busca evidenciar la necesidad que tiene el estado español de cooperar con otros países y organizaciones, ya que se estima que ni la Unión Europea ni ningún otro Estado por si solos pueden encontrar actualmente una respuesta efectiva a las amenazas a las que se enfrenta.

Trataremos también el asunto del terrorismo desde el punto de vista de la Unión Europea, es decir, desde el marco europeo y pertenencia a la OTAN, analizaremos las modificaciones en sus directivas, estrategias y las reacciones sociales al respecto.

Pistas de la propuesta.

Los progresos tecnológicos e informáticos han sido considerados un gran avance en nuestra sociedad. Debemos plantearnos esto como un fenómeno muy

positivo, pero no debemos dejar de lado el gran abanico de desventajas y oportunidades que se pueden generar para el mundo delictivo.

De estas desventajas delictivas, gran parte de ellas están consideradas como actos de tratamiento penal, “en concreto, el Derecho Penal tiene que prestar protección a nuevos valores concernidos por la implantación de los sistemas informáticos en los diversos sectores de la comunidad (personal, social, profesional, económico, financiero) y, también, ofrecer tutela a valores clásicamente amparados por el orden penal frente a nuevas modalidades de ataque derivadas del uso de los dispositivos telemáticos” (SUBIJANA, 2008, p. 170).

Nuestro estudio se centra en las acciones delictivas fruto de las desventajas que hoy por hoy más preocupan a las naciones y sus cuerpos de seguridad, todas aquellas acciones desempeñadas por grupos u organizaciones terroristas, en territorios estratégicamente ubicados, con el objetivo de hacer daño a las naciones y que hoy por hoy fundamentalmente, están dirigidas y controladas desde el espacio cibernético. Esto gracias a “una sociedad de funcionamiento en red, en la que la velocidad, la ubicuidad, la virtualidad y la transversalidad sustituyen a la territorialidad, la rigidez y la jerarquización” (SUBIJANA, 2008, p. 170).

Cuando hablamos de ciberterrorismo lo hacemos en sentido amplio y hablamos tanto de las acciones terroristas perpetradas a través de Internet como de todas aquellas gestiones o actuaciones que realizadas en este medio sirven de puente para poder llegar a realizar acciones terroristas de todo tipo e índole.

El terrorismo en la actualidad no se puede entender sin el uso de las tecnologías cibernéticas es decir el ciberterrorismo es una problemática que afecta a la seguridad mundial. Las Naciones han desarrollado estrategias jurídicas para castigar y prevenir este tipo de delitos, que ponen en entre dicho la seguridad nacional.

En el caso de España:

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.

Cuando hablamos de ciberterrorismo, hacemos referencia a los términos cibercrimen, ciberdelito o ciberdelincuencia, todos estos son delitos cometidos en el espacio virtual y presentan cuatro aspectos que los caracterizan:

1) Se cometen fácilmente.

2) Requieren escasos recursos en relación al perjuicio que causan.

3) Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.

4) Se benefician de las lagunas de punibilidad que pueden existir en determinados (SUBIJANA, 2008, p. 171).

Este tipo de crimen utiliza las tecnologías de la información para coaccionar, intimidar, causando daños a grupos sociales con fines políticos, económicos, religiosos entre otros, "el ciberterrorismo, por lo tanto, se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de medios provenientes de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa" (SUBIJANA, 2008, p. 172).

Esto nos lleva a entender la emergente y creciente necesidad que existe de generar estrategias que van encaminadas a la compenetración de cuerpos de seguridad, cooperación y unidad de esfuerzos gubernamentales para el tratamiento de este problema tan complejo, que afecta de manera directa a la seguridad nacional, social y económica.

Tenemos que destacar y ampliar en este punto, en el caso de estado español, la estrategia de Seguridad Nacional del 1 de diciembre de 2017, **"**junto a los riesgos y amenazas, conviven en el escenario internacional otros factores potenciadores que pueden generar nuevos riesgos o amenazas o multiplicar y agravar efectos. La pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos, el cambio climático o la generalización del uso nocivo de las nuevas tecnologías son algunos de esos factores".

Esta estrategia nos enumera y describe el conjunto de riesgos y amenazas para el estado español, ámbitos de actuación (Defensa nacional; Lucha contra el terrorismo; Lucha contra el crimen organizado; No proliferación de las armas de

destrucción masiva; Contrainteligencia; Ciberseguridad; Seguridad marítima; Seguridad del espacio aéreo y ultraterrestre; Protección de infraestructuras criticas; Seguridad Económica financiera; Seguridad Energética; Ordenación de flujos migratorios; Protección ante emergencias y catástrofes;, Seguridad frente a Pandemias y Epidemias; Protección del medio ambiente) y sus líneas estratégicas.

De este conjunto de riesgos y sus líneas de actuación estratégicas en nuestro trabajo nos centramos en la lucha contra el terrorismo y la ciberseguridad.

CAPÍTULO I

CIBERTERRORISMO: ANTECEDENTES, ESTRATEGIA Y CAPACIDADES OPERATIVAS ESPAÑOLAS

Iniciamos este estudio definiendo los conceptos fundamentalesque nos permitirán realizar con precisión el abordaje de cada uno de los puntos de interés para nuestra investigación, así como su evolución y transformación.

Para comenzar a hablar de **ciberterrorismo** y terrorismo apoyado cibernéticamente debemos plantearnos su origen en el nacimiento de Internet en 1969. Está considerado como el conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP *(transmisión control protocol/internet protocol),* lo quegarantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcancemundial. Es interesante recordar que “la red de redes nació de la idea y de la necesidad de establecer múltiples canales de comunicación entre ordenadores” (CHICHARRO LÁZARO 2009, p.4) y que “el advenimiento de internet y su expansión han demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea" (CARLINI 2016, p.3), pero con el desarrollo de las tecnologías de la información también se abrió una compuerta para la comisión de delitos a través de las mismas.

Este fenómeno fué tan revolucionario que en unos pocos años se produjo un enorme incremento en el número de usuarios de internet. “En 1993 se estimaba que había 14 millones y en julio de 2014 rondaban los 2900 millones” (CARLINI 2016, p.3). En la actualidad, todas las sociedades y los ciudadanos que

lasconforman, tienen una dependencia casi total de los sistemas informáticos para todos los procesos económicosy sociales, que además están íntimamente relacionados. Este rápido y acelerado crecimiento de las tecnologías de la información abrió espacios para el delito, poniendo un arma de gran calibre en manos de los delincuentes y terroristas.

De acuerdo con CHICHARRO LÁZARO (2013) "Históricamente las leyes penales surgen como respuesta a las actividades que producen daño a la sociedad y con la aparición de los ordenadores, comenzaron a emerger nuevos delitos y la preocupación por castigar ciertas conductas, recibiendo el nombre de delitos informáticos o cibercrímenes". Desde esta misma óptica "*la guerra moderna de la información lleva consigo muchas preocupaciones jurídicas: qué leyes existentes son relevantes para este nuevo modelo de guerra y cómo se pueden implementar para poder limitar los ataques cibernéticos y el ciberterrorismo. El espacio cibernético es un dominio artificial que se diferencia de los otros cuatros dominios de guerra (tierra, aire, mar y espacio). Aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. El ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, como por ejemplo las redes eléctricas. Por lo tanto, esta interconexión tendrá repercusiones graves sobre las estrategias de seguridad nacionales e internacionales"* (CARLINI, 2016).

La anterior tesis citada es apoyada por URUEÑA CENTENO (2015). Este autor define los ciberataques como "l*a mayor amenaza actual".* Precisamente por esa interconexión del mundo y de dependencia informática, donde "*cualquier fallo o intrusión en un sistema informático puede causar daños irreparables".*

Analizando los alcances e implicaciones de los medios informáticos en las acciones delictivas, es pertinente acotar la definición de *ciberterrorismo* mediante un recorrido por el término:

Para URUEÑA CENTENO (2015), un delito informático o **ciberdelincuencia** es, toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Muchos de esos delitos al no estar tipificados por la ley se definen como abusos informáticos. Una de las formas de ciberdelincuencia es el ciberterrorismo. En la

actualidad casi la totalidad de las acciones terroristas están apoyadas cibernéticamente o utilizan en algún momento medios cibernéticos en su realización bien para comunicación o acción.

SUBIJANA ZUNZUNEGUI (2008, p. 171) agrupa los términos ***cibercrímen,*** ***ciberdelito*** *o* ***ciberdelincuencia*** y "hace referencia a los delitos cometidos en el espacio virtual" identificando cuatro aspectos característicos:

- "Se cometen fácilmente.
- Requieren escasos recursos en relación al perjuicio que causan.
- Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.
- Se benefician de las lagunas de punibilidad que pueden existir en determinados Estados, algunos de los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas".

Este mismo autor cataloga de forma independiente el ciberterrorismo definiéndolo como: "cualquier acto realizado a través de tecnologías de información que pueda lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción delsoporte tecnológico de cualquiera de sus infraestructuras fundamentales" (SUBIJANA ZUNZUNEGUI, 2008, p. 173).

Cabe esperar por su grado de importancia que las autoridades mundiales encargadas de defender y aplicar las leyes enciendan sus motores, para evitar y perseguir este tipo de delitos.

CHICHARRO LÁZARO (2013) define ciberterrorismo como: "una conducta ilícita, en la que un componente esencial es la utilización de ordenadores como instrumentos o como objetivos para que se dé el tipo penal de terrorismo (CONWAY, 2003, p. 5), es decir, el propósito tiene que ser generar terror o miedo generalizado (esto es porque hay una amenaza de muerte o destrucción a gran escala) y debe sumarse una motivación política".

En este sentido, el Consejo de Europa[1] define el ciberterrorismo como la forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines político-religiosos.

En general la ciberdelincuencia y el ciberterrorismo buscan desestabilizar las estructuras sociales establecidas. España fue el tercer país, tras Estados Unidos y el Reino Unido, que mayor número de ataques cibernéticos sufrió en 2014, según declaraciones del ministro de Asuntos Exteriores, con más de 70.000 ciberincidentes, de los que no detalló la gravedad[2]. Por tanto, los crímenes del ciberterrorismo, cuando tienen la intención de causar pánico colectivo, (una alarma social generalizada), responden a una motivación ideológica determinada y conllevan implicaciones más graves que los delitos comunes para la seguridad nacional y la política de defensa (CHICHARRO LÁZARO, 2013).

En los siguientes capítulos, ampliaremos las definiciones de ciberterrorismo y revisaremos las propuestas y las normativas de los estados para afrontar la criminalidad y una adecuada respuesta ante la misma.

I.1.- ORÍGENES Y APARICIÓN

Centrándonos en el origen y aparición de los ciberataques, y posteriormente el ciberterrorismo, PONCE (2012) considera que “el advenimiento de la Web 2.0 revoluciona el concepto de red”, donde todos compartimos información que es actualizada constantemente. También menciona que “la Web 2.0 se ha llamado en muchas ocasiones como la Web social y los medios de comunicación que ofrece, también han incorporado este adjetivo, denominándose Medios Sociales o Social Media”.

Internet y la web 2.0, tal como se mencionó anteriormente, trajo consigo la aparición de actividades delictivas, que tienen la característica, como indica

[1] SUBIJANA ZUNZUNEGUI, I. J. (diciembre de 2008). El ciberterrorismo: una perspectiva legal y judicial. *Eguzkilore*, *Cuaderno del Instituto Vasco de Criminología*. (22), pp. 169-187. Recuperado de: http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

[2] GONZÁLEZ, M. (5 de febrero de 2015). “España es, tras EEUU y Reino Unido, el país que sufre más ciberataques. *El País*. Recuperado de: http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html

URUEÑA CENTENO (2015), de que "el ataque se puede realizar desde cualquier parte del mundo, lo que ofrece al ciberdelincuente varias ventajas". Si analizamos estas ventajas podemos indicar lo siguiente: el ciberatacante se siente seguro, ya que no se expone físicamente a su víctima ni mucho menos a la posible intervención de las fuerzas de seguridad, dado que su acción delictiva se realiza *a distancia*; sensación de cómoda impunidad, al saber que hay lagunas legislativas a nivel internacional, por lo que muchos de los delitos cometidos no *se castigan*; el delincuente aprovecha el anonimato de sus ciberacciones al ser complicado identificar al atacante; cualquier usuario que tenga un equipo informático y conexión a internet, con unos conocimientos técnicos que están al alcance de cualquiera y con una inversión económica no elevada, puede ejecutar un ciberataque; cualquier ciberataque conlleva un efecto de vulnerabilidad y falta de protección individual; y por último estos ataques sacuden la opinión pública y tiene gran difusión en los medios digitales de todo el mundo.

Determinando que el origen del ciberterrorismo radica en su raíz misma como espacio cibernético, éste es por tanto, el escenario donde se desarrollan las amenazas cibernéticas. Hemos tomado la conceptualización del mismo emanada del Departamento de Defensa de los EE.UU.: el *ciberespacio* sería *"Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores"* (RUIZ DÍAZ, 2016).

La Comisión Europea define el **ciberespacio** como "el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo", término que se utiliza actualmente para describir toda la gama de recursos de información disponible a través de redes informáticas[3].

Por último la UIT (Unión Internacional de las Telecomunicaciones) define el ciberespacio como "el lugar creado a través de la interconexión de sistemas de ordenador mediante Internet" y ciberseguridad como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión

[3] Vid. EUROPEAN COMMISSION. (2018). Glossary and Acronyms. Recuperado de: http://ec.europa.eu/idabc/en/document/651/5892.html

de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio"[4].

Desde esta conceptualización, según el mismo RUIZ DÍAZ (2016), el uso del ciberespacio en el entorno terrorista ha experimentado un importante crecimiento que se mantiene constante sobre un medio, como Internet, que se ha demostrado vulnerable. En consecuencia, la red de redes se ha convertido tanto en un instrumento, como en un medio para los terroristas: Un instrumento para la captación, la radicalización y acción-realización de actos terroristas y un medio de propaganda de estos actos terroristas.

I.2.- EVOLUCIÓN

Entender la **ciberdelincuencia** conlleva definirla en el marco espacial que la sostiene. SUBIJANA ZUNZUNEGUI (2008, p. 171) lo describe así: "La comisión de un ciberdelito suele producirse en el marco de una relación cuadrangular. El sujeto activo (A), de quien parte la acción de insertar en la red una información destructiva o un dispositivo pernicioso, persona que se sirve, para tal fin, de un ordenador. Los coadyuvantes no intencionados, que son el proveedor de servicios de Internet (B) que conectará al usuario, a través de la línea telefónica en Internet y el servidorweb (C) donde se aloja, en un disco duro, la información destructiva o el dispositivo pernicioso por el cual se materializa la acción delictiva antijurídica. Este servidor puede coincidir con el proveedor de servicios de Internet. El sujeto pasivo del delito (D), que es quien padece los daños derivados de la información destructiva o el dispositivo pernicioso y que, en muchas ocasiones, es indeterminado, desconocido e internacional".

Esta relación cuadrangular es usada por las organizaciones terroristas para el cumplimiento de sus objetivos estratégicos. Empleancuidadosas estrategias de marketing, una adecuada utilización de las redes sociales virtuales, que también

[4] Vid UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. Ref. UIT-T X. 1205. Recuperado de: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

es empleada para conseguir recursos económicos y de otras índoles, a fin de realizar su cruzada armamentista. Los diversos acontecimientos acaecidos han llevado a los diversos autores y estudiosos en materia de ciberterrorismo aun consenso: Actualmente los ciberataques en sus diferentes modalidades, entre las que se encuentra el ciberterrorismo, representan una amenaza cada vez mayor no solo para el individuo, sino también para la sociedad en su conjunto. Tanto es así, que se considera que los "Ciberataques son hoy en día la estrategia de guerra más poderosa" (URUEÑA CENTENO, 2015).

Por tanto, el **ciberterrorismo** analizado desde la perspectiva de SUBIJANA ZUNZUNEGUI (2008, p. 172), "puede ser visto desde una óptica medial o final. La perspectiva medial tiene como referente el aprovechamiento por los grupos terroristas de las posibilidades que brindan las nuevas tecnologías de la información y de la comunicación para la consecución de sus fines deletéreos. Constituye una forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos o religiosos, básicamente. Desde esta perspectiva medial, el ciberterrorismo, por lo tanto, se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de medios provenientes de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa".

A raíz de esto, el Consejo de Europa en su Convenio sobre la ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest y ratificado por España en el año 2010, engloba las actuaciones de ciberdelincuencia y tipifica las diversas actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza serían constitutivos de delito. Un breve resumen de los mismos, sería el siguiente[5]:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: Acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema y abuso de los dispositivos.

[5] RUIZ DÍAZ, J. (22 de octubre de 2016). Ciberamenazas: ¿el terrorismo del futuro? *(DIEEEO86-2016)*. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

- Delitos informáticos, entre ellos: Falsificación informática o fraude informático.

- Delitos relacionados con el contenido: Pornografía infantil (producción, puesta a disposición, difusión, adquisición o posesión de la misma por medio de un sistema informático).

- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[6].

Nuevamente RUIZ DÍAZ (2016) en su análisis de las ciberamenazas como terrorismo advierte que, las consecuencias mássignificativas de este tipo de delitos son las económicas y las de reputación, aunque por supuesto no debemos restar importancia a los relacionados con el contenido, los cuales suponen un ataque a la dignidad y los derechos fundamentales de las personas. Los ataques son cada vez más sofisticados y afectan redes informáticas que, en teoría, disponen de niveles de seguridad extremos. Es entonces cuando en este análisis de las implicaciones de los ciberataques, aparece un factor económico, que definido como "inteligencia económica representa el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico. Acciones que se dirigen tanto al ámbito de la economía nacional como en el dominio empresarial, pues la globalización de los mercados pone también en riesgo a las propias empresas"[7].

En el mismo orden de ideas se hace presente otro fenómeno delictivo, **el ciberespionaje**, el cual con amplia incidencia en el sector económico afecta principalmente a las grandes empresas multinacionales que sufren igualmente el acoso de los espías electrónicos, en busca de información sobre nuevos proyectos de desarrollo, dentro de un entorno altamente globalizado y competitivo (RUIZ DÍAZ, 2016).

[6]JEFATURA DEL ESTADO. ESPAÑA. (17 de septiembre de 2010). Instrumento de ratificación del Convenio sobre Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. *Boletín Oficial del Estado (BOE)* Nº. 226., Sec. I. Pp. 78847-78896. Recuperado de: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

[7]OLIER, E. (2013). "Inteligencia estratégica y seguridad económica", en *Cuadernos de Estrategia* 162. La inteligencia económica en un mundo globalizado. Instituto Español de Estudios Estratégicos. IEEE. Ministerio de Defensa. 2013, pp. 9-31. (Ver p. 11).

Entre los delitos tipificados como ciberdelincuencia encontramos: el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos. Muchos de éstos son delitos que se configuran bajo el manto de los conflictos bélicos que utilizan como campo de batalla el ciberespacio y las tecnologías de la información con el único fin de inhabilitar los sistemas informáticos de los enemigos y obtener información.

Todos estos actos de ciberataques, dependiendo del daño que se quiera provocar y los objetivos del mismo, utilizan diversas técnicas e instrumentos que son aplicados conjuntamente o de forma individualizada. Entre éstas están[8]:

- Los virus informáticos: Los Virus Informáticos son esencialmente programas de carácter malicioso, que pretenden infectar archivos contenidos en el sistema, con el objeto de producir modificaciones o daños en el sistema informático que han infectado. El archivo infectado con el virus, se denomina "víctima". El virus introduce en los archivos infectados una secuencia de código malicioso, dirigida fundamentalmente a los archivos ejecutables del sistema atacado. A cada ejecución de estos archivos, se produce una propagación del virus, infectando a nuevos archivos y multiplicando sus efectos.

- El envío masivo de correo no deseado o SPAM: Se llama "*Spam*" a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente con publicidad, generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *"spamming".* Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Esta técnica también puede tener como objetivo los teléfonos móviles, a través de mensajes de texto o con los sistemas de mensajería instantánea.

- La suplantación de remitentes de mensajes mediante *Spoofing*: La idea de este ataque, otra cosa es la puesta en práctica, es *muy* sencilla: desde su

[8] URUEÑA CENTENO, F. J. (2015). Ciberataques, la mayor amenaza actual. Documento de Opinión nº 09/2015. Instituto Español de Estudios Estratégicos. Madrid: IEEE.

equipo, un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del *host* suplantado. Utilizando comandos del sistema, los accesos NFS, o la protección de servicios de red mediante TCP *Wrapper*, el *spoofing* sigue siendo en la actualidad un ataque peligroso y factible contra cualquier tipo de organización.

- El envío o instalación de archivos espías o *Keyloggers*: Como su nombre indica un *Keylogger* es un programa que registra y graba la pulsación de teclas y, algunos, también los clicks del ratón. La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (*software*) que realizan estas tareas.

- El uso de Troyanos para el control remoto de los sistemas o la sustracción de información: Los Troyanos Informáticos o Caballos de Troya son una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos habituales (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. El objetivo principal de un Troyano Informático es crear una puerta trasera (*backdoor* en inglés) que dé acceso a la administración remota del equipo infectado, con el objeto de robar información confidencial y personal. Las acciones que el atacante puede realizar dependen de los privilegios del usuario que está siendo atacado y de las características del troyano. Como ejemplos de troyanos tenemos *Back Orifice 2000, SubSeven, Cybersensor, DeepThroat v2, Dolly Trojan, Girlfriend, nCommand v1.0, NetSpher*, etc.

- El uso de archivos BOT del IRC (Internet *Relay Chat*): es una contracción de la palabra robot. Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario. En webs de conversación *online* como por ejemplo los *chats* o programas IRC, algunos bots son utilizados para simular una persona y hacer un uso maligno, intentando hacer creer a los demás usuarios del servicio que hablaban con una persona real. Pero la utilización efectiva para el

cibercrímen es el mantenimiento de salas de chat, abiertas indefinidamente, y que son utilizadas esporádicamente como canal de comunicación. Al tener un BOT funcionando continuamente, el IRC detecta a ese BOT como a una persona activa en el chat, por lo que esa sala de chat nunca es clausurada.

- El uso de *Rootkits*: Es un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Los *rootkits*, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el *rootkit* mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

RUIZ DÍAZ (2016, p. 5) describe los tipos de ataques presentados con las técnicas descritas anteriormente, bien sea usadas individualmente o en conjunto, provocando los siguientes efectos:

- Cambios en las direcciones de dominio (DNS): El cambio de dominio significa que la web o un servicio determinado va a tener otra dirección, por lo que los usuarios o el mismo propietario no tendrían acceso a un determinado recurso, provocando un grave perjuicio, dependiendo del ámbito de dicho servicio.

- Intrusiones no autorizadas: A día de hoy, es rara la estación de trabajo que no está conectada a Internet. La posibilidad de acceder remotamente a los equipos abre la puerta para los accesos maliciosos por parte de personas no autorizadas. Una intrusión puede tener básicamente dos efectos negativos: la filtración de información confidencial, y la destrucción de datos por parte del intruso.

- En el caso de la destrucción, se puede deber al deseo de reconocimiento social o por otros motivos (conflictos políticos entre países, sabotaje industrial, etc.).

- DDoS (Denegación de servicio): DDoS son las siglas de *Distributed Denial*

of Service. La traducción es “ataque distribuido de denegación de servicio”. Se ataca al servidor desde muchos ordenadores para que deje de prestar servicio.

- El DDoS es un método relativamente sencillo, de hecho, valdría con que hubiese un número suficientemente grande de personas solicitando simultáneamente servicios de una web para colapsarla. Sin embargo, las herramientas que se suelen usar son algo más sofisticadas. Con ellas se pueden crear muchas conexiones simultáneas o enviar paquetes alterados para multiplicar los accesos. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real.

- Otra técnica para llevar a cabo los DDoS es usar *botnets*: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que está participando en un ataque DDoS, por lo que es más difícil encontrar al verdadero atacante.

- Saturación de correos: consiste en enviar masivamente emails a un servidor o una cuenta, de tal forma que éste se sature por la gran cantidad de datos que recibe y que llegan al límite de almacenamiento o de su capacidad de procesamiento, impidiendo la recepción y envío de los emails reales y necesarios.

- Interferenciaelectrónica de comunicaciones: La interferencia electromagnética es la perturbación que ocurre en cualquier circuito, componente o sistema electrónico causado por una fuente de radiación electromagnética externa al mismo. También se conoce como EMI por sus siglas en inglés *(Electro Magnetic Interference), Radio Frequency Interference o RFI*. Esta perturbación puede interrumpir, degradar o limitar el rendimiento de ese sistema. La fuente de la interferencia puede ser cualquier objeto, ya sea artificial o natural, que posea corrientes eléctricas que varíen rápidamente, como un circuito eléctrico, el sol o las auroras boreales.

- En el tema que nos ocupa, se trata de interferencias causadas por señales emitidas intencionadamente, con el propósito expreso de producir una disfunción en los sistemas de comunicaciones, es decir, una interferencia. El dispositivo más común es el inhibidor de frecuencias. Un inhibidor de frecuencias es un dispositivo capaz de dificultar o impedir las comunicaciones por radiofrecuencia entre otros dispositivos que están en su campo de alcance. Sirve para interrumpir la señal entre teléfonos móviles, redes WiFi, walkie talkies o bluetooth. Su objetivo no es eliminar o suprimir determinadas frecuencias del espectro sino producir un ruido mayor que imposibilite que emisor y receptor puedan entenderse en su proceso comunicativo. El inhibidor de frecuencias está formado por un generador de onda y un transmisor. En conjunto, generan y emiten una señal de mayor potencia que la del resto de dispositivos.

- BlindRadars, bloquear tráfico aéreo: Se trata de una técnica de interferencia electrónica de los radares de las torres de control y de los sistemas de seguimiento de aeronaves. Mediante esta técnica los centros de control de tráfico aéreo, pierden la localización exacta de los aviones, por lo que los controladores aéreos no pueden desarrollar su labor y no pueden guiar a las aeronavesen su ruta de viaje y en los despegues y aterrizajes, pudiéndose producir choques en el aire o que el avión se estrelle en su maniobra de aproximación a la pista de aterrizaje.

- Ataque por robo de información: Más del 40% de los programas maliciosos que se envían vía e-mail tienen como finalidad robar información personal y financiera. Muchos de ellos son dirigidos a empresas. Con el surgimiento del modelo de negocio *online*, fueron apareciendo nuevos y cada vez más complejos ataques informáticos que buscan obtener información confidencial de los usuarios, dando lugar a una nueva modalidad delictiva, encuadrada dentro del marco de las estafas.

- De los principales métodos actuales para obtener información personal de usuarios, el primero de ellos es el *phishing*. El *phishing* es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente involuntaria y fraudulenta, datos

personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social.

- El segundo, son los códigos maliciosos como *backdoor, keylogger* o los troyanos bancarios (*bankers*).

- Ataque por anulación de equipos: Mediante el envío de virus se puede conseguir que equipos personales o servidores queden paralizados para dar el servicio requerido. Este tipo de ataque provoca unos síntomas comunes en los equipos atacados, como que el equipo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia, se reinicia cada pocos minutos, las aplicaciones del equipo no funcionan correctamente, o no se puede obtener acceso a determinados dispositivos o pantallas distorsionadas.

- Ataque por pulso electro-magnético: El ataque de pulso electromagnético es un método de ataque militar realizado con armas generadoras de importantes cantidades de energía electromagnética ambiental que destruyen total o parcialmente el equipamiento eléctrico y electrónico dentro de su radio de acción. Un EMP es un pulso de energía que puede estar generado por fuentes naturales como rayos o tormentas solares que producen ionizaciones en la atmósfera de la Tierra, la ionosfera y el campo magnético, o también puede ser creado artificialmente mediante un arma nuclear u otros dispositivos no-nucleares. El pulso electromagnético (o EMP en sus siglas en inglés) es un efecto secundario descubierto con las pruebas atómicas. Se observó que, tras una explosión nuclear, los aparatos electrónicos en un cierto radio de acción quedaban dañados o totalmente inutilizados.

- Las posibilidades que ofrece este fenómeno en el campo de la ciberguerra son inmensas. Los ingenieros militares se dieron prisa en desarrollar artefactos que maximizaran dicho efecto. Una bomba EMP detonada cerca de fuerzas enemigas dejaría todas sus defensas y contramedidas en tierra inmovilizadas y más teniendo en cuenta que la ventaja que hoy en día confiere la electrónica a los ejércitos modernos es vital. Pero ésta no es la

única estrategia posible. Existe lo que se llama ataque de pulso electromagnético de gran altitud o HEMP, capaz de paralizar un continente entero con un solo disparo.

En el ámbito jurídico este tipo de ataques cibernéticos pueden clasificarse de la siguiente forma según acuerdo contemplado en la carta de las Naciones Unidas[9] como principal fuente de *jus ad bellum* (CARLINI, 2016):

- "Uso de la fuerza". Son ataques patrocinados por los Estados contra otro Estado.Estos violan el artículo 2 de la Carta de las Naciones Unidas, provocando un conflicto armado internacional.

- "Ataques armados". Se presentan cuando un estado desarrolla operaciones cibernéticas contra otro estado. Por lo tanto, el Estado atacado tiene el derecho de legítima defensa (el artíc. 51 de la Carta de las NNUU reconoce el derecho a la legítima defensa), de otra manera prohibido por la Carta de las Naciones Unidas.

- "Actos de agresión y amenaza a la paz". Así son considerados los ataques cibernéticos. Por lo tanto, el Consejo de Seguridad debe entrar a restablecer la seguridad y la paz internacional.

CARLINI[10], profundiza sobre estos ataques cibernéticos como "uso de la fuerza" por lo quedebería tomarse en consideración el instrumento, el objetivo y un enfoque basado en los efectos. Considera que el más relevante es un enfoque basado en efectos, y toma para tal fin el trabajo realizado por el Grupo de Expertos del Manual de Tallin, que concluye que: *«los actos que lesionan o matan personas, que dañan o destruyen objetos son inequívocamente uso de la fuerza»* y que *«ataques cibernéticos no destructivos cuya finalidad es perjudicar la estabilidad económica y gubernativa de un Estado no se califica como «uso de la fuerza»*[11]. El manual enumera ocho factores (propuestos anteriormente por MICHAEL N.

[9] ONU. (1945). Carta de las Naciones Unidas. Recuperado de: http://www.un.org/es/sections/un-charter/chapter-i/index.html

[10] CARLINI, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. Instituto Español de Estudios Estratégicos, p. 8. Madrid: IEEE. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

[11] MICHAEL N. SCHMITT, M. N. (ed). (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press 2013, p. 45.

SCHMITT en 1999) esenciales para determinar si una operación cibernética puede o no ser clasificada como «uso de la fuerza». Estos factores consisten en: invasividad, severidad, carácter militar, inmediatez, participación estatal, cuantificación de los efectos, presunta legalidad y franqueza (CARLINI, 2016, p. 9). En ese orden de ideas, para este grupo de Expertos, una operación cibernética cuenta como «uso de la fuerza» cuando produce el mismo nivel de daño físico a objetos y personas que las *Kinetic Operations*[12].

En general el cibercrimen ha crecido en todas las naciones, pero en España se ha producido un incremento "bestial" de este tipo de crimen: se pasa de 35.000 delitos registrados en el año 2011 a 66.584 en 2016. Este tipo de medios son cada vez más utilizados por la delincuencia (espionaje, sabotaje, robo de información, ataques…). El propio director de Europol afirma que ésta es una amenaza real, constante y creciente, siendo la piedra angular de este crímen la difusión del malware.

Igualmente, DAVID BARROSO director ejecutivo de *Countercraft*[13] opina: que *"contra el ciberdelincuente, poco se puede hacer. Las reglas que nos vamos inventando, van quedando obsoletas según los criminales encuentran el modo de sortearlas",* no podemos cerrar los ojos, debemos trabajar conjuntamente unos países con otros, los legisladores con las fuerzas de seguridad, solo la coordinación y cooperación nos harán fuertes ante el ciberdelincuente. También propone como experto dosmandamientos básicos[14]:

- *Si algo huele mal, seguramente es peligroso.*
- *Cuando metemos algo en internet, deja de pertenecernos."*

Somos el noveno país en Europa con más delitos de este tipo, tres puntos por encima de la media. De 66.584 delitos conocidos en 2016 se esclarecieron 20.452 y sólo 4.799 acabaron en detenciones. Faltan muchos medios tanto

[12] Entiéndase como aquellas medidas militares que impliquen la fuerza letal, básicamente tácticas de guerra.

[13] CounterCraft, compañía de contrainteligencia en el ámbito de la ciberseguridad, ha desarrollado una solución que utiliza técnicas y herramientas de engaño para detectar, descubrir y manipular a los adversarios.Vid. https://www.countercraft.eu/company.html

[14] HIDALGO PÉREZ, M. (19 de diciembre de 2017). Seguridad. España tiene perdida la guerra contra el cibercrimen. *El País*, Madrid. Recuperado de: https://retina.elpais.com/retina/2017/07/11/tendencias/1499762151_884595.html

técnicos como humanos. Además, muchos de estos delitos no llegan a denunciarse.

Según este estudio podemos ver que el 87% de los delitos esclarecidos son realizados por españoles, un total de 4799, seguidos de 294 realizados por ciudadanos rumanos y 24 por ciudadanos del Reino Unido. Para poder lograr esclarecer este tipo de delito las fuerzas de seguridad necesitan contar con una legislación ágil y las mejores herramientas, siendo una buena estrategia la cooperación entre las fuerzas de seguridad y los fabricantes de tecnología.

Este tipo de actos y la dificultad para su tipificación en materia jurídica ha obligado a las naciones a actualizar los conceptos de Seguridad y Defensa debido a las diversas razones que han producido un incremento del Riesgo[15], entre éstas encontramos:

- La diversificación de actores (o activos que son potenciales objetivos) dentro de la Seguridad y la Defensa:
  - Organizaciones públicas, tanto civiles como militares.
  - Organizaciones privadas.
  - Ciudadanos.

- La diversificación y el aumento de las amenazas:
  - Los terroristas y las organizaciones criminales.
  - Las naciones hostiles, el personal descontento.
  - Las catástrofes naturales.
  - El simple ciudadano que persigue salir en los medios de comunicación.

Los riesgos que se mencionan en el párrafo anterior están asociados a las vulnerabilidades de los sistemas. De acuerdo con la Escuela de Altos Estudios de la Defensa Española, éstas se pueden definir como “cualquier debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas”. Las vulnerabilidades no solamente son características inherentes a la naturaleza de sus activos; también se considera una vulnerabilidad la presencia de errores de

[15] Riesgo: estimación del grado de exposición a que una amenaza se materialice, a través de las vulnerabilidades, sobre uno o más activos causando daños o perjuicios sobre los mismos.

diseño, implementación, operación o administración de un sistema de información que puedan ser explotados y deriven en un efecto no deseado o no esperado que comprometa la directiva de seguridad del sistema[16].

La Escuela de Altos Estudios sostiene igualmente que: "Una misma vulnerabilidad afecta de manera diferente al nivel global de riesgo de una organización. Esto depende de factores como la facilidad con la que ésta pueda ser explotada o el propio activo ser alcanzado por un atacante dentro de la organización. También del valor del propio activo o de si existen contramedidas en la organización que eviten la materialización de amenazas sobre esa vulnerabilidad"[17]. Estos riesgos y vulnerabilidades los podemos observar mejor en la ilustración 1:

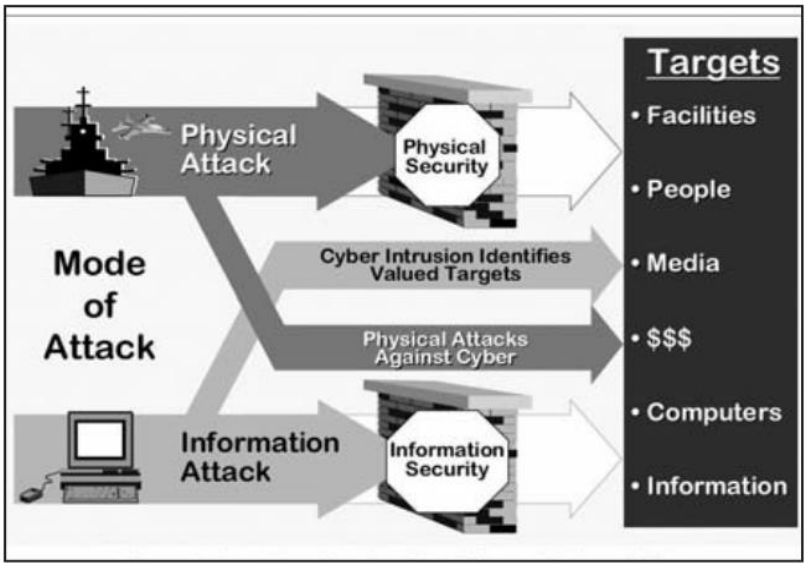


***Ilustración 1**: Nuevos riesgos y vulnerabilidades[18].*

Estas vulnerabilidades y riesgos asimismo parten del desarrollo y la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en todos los sectores, tanto públicos como privados, aumentando su dependencia de las TIC y por tanto el grado de vulnerabilidad con respecto a estas tecnologías.

[16] ESCUELA DE ALTOS ESTUDIOS DE LA DEFENSA. (Junio de 2014). Estrategia de la información y seguridad en el ciberespacio. Documentos de Seguridad y Defensa nº 60, p. 31. Recuperado de: https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf

[17] Ibídem, p. 31

[18] PASTOR ACOSTA, O. PÉREZ RODRÍGUEZ, J.A. ARNÁIZ DE LA TORRE, D. Y TABOSO BALLESTEROS, P. (2009). Seguridad nacional y ciberdefensa. Recuperado de: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

Otro aspecto relevante de estas últimas es su aspecto facilitador, lo que permite a las potenciales amenazas traspasar las fronteras nacionales y continentales y actuar a veces de forma anónima (PASTOR ACOSTA, et al, 2009).

"No debemos olvidar, sin embargo, la advertencia que se contiene en el Informe preparado por el Comité Internacional de la Cruz Roja" este termina "salvo los pocos actos específicos de terrorismo que pueden tener lugar en un conflicto armado, la opinión es que el término 'acto de terrorismo' debería utilizarse exclusivamente para los actos de violencia cometidos fuera de un conflicto armado"[19].

Para contrarrestar los riesgos y vulnerabilidades, los estados toman las medidas necesarias, pero éstos no pueden tomar acciones fuera de los pactos internacionales, bajo el amparo de Naciones Unidas, retomando el aspecto relacionado con el uso de la fuerza el artículo 2(4) de la Carta de la ONU que versa:

"Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

Sin embargo, el uso de la fuerza debe imputarse a un Estado concreto, incluso cuando estas acciones estén realizadas por personas o agentes del Estado que es responsable internacionalmente por sus conductas. Esas personas o entidades, cuyo vínculo con un Estado no es lo suficientemente claro y que hace imposible empezar un proceso internacional sobre la responsabilidad estatal, se califican como «actores no estatales». Las acciones cibernéticas realizadas por los actores no estatales o *hackers* privados se consideran bajo el Derecho Humanitario Internacional y el Derecho Penal Internacional (CARLINI, 2016).

Aun así, los Estados afectados deben responder mediante su Derecho Penal Nacional antes de tomar en consideración una intervención del Consejo de

[19] VALLES CAVIAS, J. A. (2017). El concepto de acto terrorista y el comportamiento de fuerzas armadas durante un conflicto armado. Comentario de la sentencia TJUE (Gran Sala) de 14 de marzo de 2017, asunto C-158/14. Revista de Derecho Comunitario Europeo, 57, 689-707. Recuperado de: https://doi.org/10.18042/cepc/rdce.57.09

Seguridad, para preservar la paz y la seguridad.

Para el caso español en lo referente a Seguridad Nacional y Ciberdefensa, no se encuentra recogido ni tipificado en leyes específicas. Son aspectos que se tratan de manera más o menos profunda dentro de la legislación (PASTOR ACOSTA, et al, 2009).

Por lo tanto, destacaríamos dentro de la normativa los siguientes aspectos:

- Leyes recogidas en la "Guía Legal de Respuesta Jurídica frente a los Ataques contra la Seguridad de la Información" publicada por el extinto INTECO (Instituto Nacional de Tecnologías de la Comunicación), en la que se relacionan las amenazas, las medidas de protección y las medidas legales relativas a los ataques.
- El conjunto de Artículos CP y Leyes que tratan de manera directa o indirecta el tema del terrorismo. Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP, en materia de delitos de terrorismo.

La Resolución 2178 del Consejo de Seguridad de Naciones Unidas, aprobada el 24 de septiembre de 2014, recoge la honda preocupación de la comunidad internacional por el recrudecimiento de la actividad terrorista y por la intensificación del llamamiento a cometer atentados en todas las regiones del mundo. En el catálogo de medidas que constituyen la parte dispositiva de esta Resolución, aparece en el punto sexto un recordatorio de la Resolución 1373 (2001), en virtud de la cual todos los Estados miembros deben velar por el enjuiciamiento de toda persona que participe en la financiación, planificación, preparación o comisión de actos de terrorismo o preste apoyo a esos actos. Tras este recordatorio, la Resolución 2178 pide a los Estados que se cercioren de que sus leyes y otros instrumentos legislativos internos apliquen la resolución 1373.

Además, que tipifiquen delitos graves que sean suficientes para que se puedan enjuiciar y sancionar las conductas terroristas que se describen, de tal forma que quede debidamente reflejada la gravedad del delito.

Las acciones terroristas a las que alude detalladamente la Resolución 2178 constituyen el máximo exponente de las nuevas amenazas que el terrorismo

internacional plantea a las sociedades abiertas y que pretenden poner en riesgo los pilares en los que se sustenta el Estado de Derecho y el marco de convivencia de las democracias del mundo entero.

El terrorismo internacional de corte yihadista se caracteriza, precisamente, por haber incorporado esas nuevas formas de agresión, consistentes en nuevos instrumentos de captación, adiestramiento o adoctrinamiento en el odio, para emplearlos de manera cruel contra todos aquellos que, en su ideario extremista y violento, sean calificados como enemigos. Estas nuevas amenazas deben, por tanto, ser combatidas con la herramienta más eficaz que los demócratas pueden emplear frente al fanatismo totalitario de los terroristas: la ley.

Este terrorismo se caracteriza por su vocación de expansión internacional a través de líderes carismáticos que difunden sus mensajes y consignas por medio de internet y, especialmente, mediante el uso de redes sociales, haciendo público un mensaje de extrema crueldad que pretende provocar terror en la población o en parte de ella y realizando un llamamiento a sus adeptos de todo el mundo para que cometan atentados.

Los destinatarios de estos mensajes pueden ser individuos que, tras su radicalización y adoctrinamiento, intenten perpetrar ataques contra los objetivos señalados, incluyendo atentados suicidas.

No menos importante es el fenómeno de los combatientes terroristas desplazados que deciden unirse a las filas de las organizaciones terroristas internacionales o de sus filiales en alguno de los escenarios de conflicto bélico en que los yihadistas están participando, singularmente, Siria e Irak. Este fenómeno de los combatientes terroristas desplazados es, en este momento, una de las mayores amenazas a la seguridad de toda la comunidad internacional y de la Unión Europea en particular, toda vez que éstos se desplazan para adiestrarse en el manejo de armas y explosivos, adquirir la capacitación necesaria y ponerse a las órdenes de los grupos terroristas.

La experiencia de la lucha contra el terrorismo en España nos ha permitido contar con una legislación penal eficaz en la respuesta al terrorismo protagonizado por bandas armadas extintas, como ETA o el GRAPO, esto es, grupos terroristas

cohesionados alrededor de uno o varios líderes, con estructura orgánica clara, reparto de roles dentro de la organización y relaciones de jerarquía definidas y asumidas por los integrantes del grupo terrorista. La respuesta penal al terrorismo se articulaba, por tanto, en la sanción de quienes pertenecían, actuaban al servicio o colaboraban con organizaciones o grupos terroristas.

El eje del tratamiento penal del terrorismo era, por tanto, la definición de la organización o grupo terrorista y la tipificación de aquellas conductas que cometían quienes se integraban en ellas o, de alguna forma, prestaban su colaboración.

El Código Penal no debe, en ningún caso, perder esa perspectiva de tipificación de las conductas articuladas en torno a organizaciones o grupos terroristas, pero es evidente que las nuevas amenazas exigen la actualización de la normativa para dar cabida al fenómeno del terrorismo individual y a las conductas que constituyen la principal preocupación de la comunidad internacional, en línea con la Resolución 2178 del Consejo de Seguridad de Naciones Unidas anteriormente citada. Esta Ley Orgánica modifica el Capítulo VII del título XXII del libro II de la Ley Orgánica 10/1995, de 23 de noviembre, CP, de tal forma que el rigor de la respuesta penal frente a crímenes tan graves contemple, además de las modalidades de terrorismo ya conocidas, las que proceden de las nuevas amenazas.

Las tres modificaciones legislativas en las que se basa la defensa legal contra el terrorismo en el estado español son las siguientes:

1. El Capítulo VII del título XXII del libro II de la Ley Orgánica 10/1995, de 23 de noviembre, CP, se divide en dos secciones y comprende los artículos 571 a 580[20].

[20] La sección 1ª lleva por rúbrica «De las organizaciones y grupos terroristas» y mantiene la misma lógica punitiva que la regulación hasta ahora vigente, estableciendo la definición de organización o grupo terrorista y la pena que corresponde a quienes promueven, constituyen, organizan o dirigen estos grupos o a quienes se integran en ellos.

La sección 2ª «De los delitos de terrorismo» y comienza con una nueva definición de delito de terrorismo en el artículo 573 que se inspira en la Decisión Marco 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, sobre la lucha contra el terrorismo, modificada por la Decisión Marco 2008/919/JAI, de 28 de noviembre de 2008. La definición establece que la comisión de cualquier delito grave contra los bienes jurídicos que se enumeran en el apartado 1 constituye delito de terrorismo cuando se lleve a cabo con alguna de las finalidades que se especifican en el mismo artículo:

2. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP*[21].*
3. Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal[22]; y de la Directiva 2014/42/UE[23].

Las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el marco de consenso de la normativa europea.

De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos.

Con el mismo planteamiento, y de acuerdo con las exigencias de la Directiva, se incluye la tipificación de la interceptación de transmisiones entre sistemas, cuando no se trata de transmisiones personales: la interceptación de comunicaciones personales ya estaba tipificada en el Código Penal; ahora se trata de tipificar las transmisiones automáticas (no personales) entre equipos.

1ª) 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.
2ª) Alterar gravemente la paz pública.
3ª) Desestabilizar gravemente el funcionamiento de una organización internacional.
4ª) Provocar un estado de terror en la población o en una parte de ella.

[21] Vid. Apartado III.1.1 (Capítulo III) de esta investigación.

[22] Vid. DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Recuperado de: https://www.boe.es/doue/2013/218/L00008-00014.pdf

[23] Vid. DIRECTIVA 2014/42/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 3 de abril de 2014 sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea. Recuperado de: https://www.boe.es/doue/2014/127/L00039-00050.pdf

Se tipifica la facilitación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos.

Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información.

Finalmente, en estos delitos se prevé la responsabilidad de las personas jurídicas[24].

Es de importancia nombrar a ALONSO[25] y sus aclaraciones acerca de la Ley Orgánica de Protección de Datos Personales (LOPD), ley que protege la información de los datos, mensajes, conversaciones etc, de los ciberusuarios que circulan por la red, actuando muchas veces como un obstáculo en las investigaciones realizadas por las fuerzas de seguridad del estado. "La protección de datos ("*habeas data*"). Este derecho dimana directamente del artículo 18.4 de la CE y está desarrollado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, que aprueba su Reglamento[26]. Las plataformas de redes sociales pueden presentar diversos riesgos en lo que a la protección de datos se refiere, ya que los datos personales de los usuarios son tratados con diferentes finalidades por dichas plataformas y lo habitual es que sean comunicados, cedidos o puestos a disposición de terceros por diversos motivos, tales como su mantenimiento por servicios de *"hosting*" (alojamiento en servidores) y almacenaje o su comunicación a terceros para llevar a cabo acciones de *marketing*. En efecto, la esencia del negocio de red social se encuentra en los datos que los usuarios proporcionan y hacen públicos a través de sus perfiles, hasta el punto de que se ha llegado a

24 Vid. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado(BOE)*, nº 77, sección 1, pp. 27061-27176.

25 ALONSO GARCÍA, J. (2015). Derecho penal y redes sociales (1ª ed.). Madrid: Aranzadi.

26 Hay que tener en cuenta el Reglamento Europeo de Protección de Datos (RGPD) tendrá aplicabilidad directa en todos los Estados miembros a partir del 25 de mayo de 2018, (dos años después de su publicación). Además, el 10 de noviembre de 2017 el Consejo de Ministros aprobó la remisión a las Cortes Generales del Proyecto de Ley Orgánica de Protección de Datos, que tiene por objeto adaptar la legislación española a las disposiciones del RGPD. El RGPD cambia radicalmente la forma actual de regular la protección de datos, obligando a empresas, organismos, instituciones y administraciones a cambios y esfuerzos significativos de carácter organizativo, técnico, económico y humano al imponer nuevas obligaciones y requerimientos.

afirmar que los usuarios de las plataformas de redes sociales no son clientes, sino producto. En palabras de JAN KOUM -fundador de la aplicación de mensajería móvil *"WhatsApp"-,* "si no eres el cliente, eres el producto" (ALONSO GARCÍA, 2015).

Por otro lado, en cuanto a los principales planes y estrategias relacionados con la Seguridad Nacional y la Ciberdefensa, los más destacados son los siguientes:

- La Revisión Estratégica de la Defensa de España del 2003, las Directivas de Defensa Nacional (DDN) emitidas en 1980, 1984, 1986, 1992, 1996, 2000, 2004, 2008 y 2012, además de la Ley Orgánica de Defensa Nacional de 2005.
- Plan Nacional de Protección de las Infraestructuras Críticas.
- Desarrollo del Centro de Alerta Temprana Antivirus (CATA).
- Desarrollo de diversos CERT´s (públicos y privados).
- Esfuerzos realizados por el CCN para la mejora de la seguridad de la información en la Administración Publica.
- MoU del 14 de mayo de 2008 para la participación de España en el Centro de Excelencia de Ciberdefensa Cooperativa.
- Estrategia Española de Seguridad[27] de 2011, diseñada desde una perspectiva nacional, pero también europea, internacional y global, como base de partida hacia la siguiente Estrategia de Seguridad Nacional "Un proyecto compartido" de 2013[28], y la última Estrategia de Seguridad Nacional "Un proyecto compartido de todos y para todos" de 2017[29].
- Estrategia de Ciberseguridad Nacional aprobada por el Consejo de

[27] PRESIDENCIA DEL GOBIERNO, ESPAÑA. (30 de junio de 2011). *Estrategia Española de Seguridad. Una responsabilidad de todos (EES).* Aprobada por el Consejo de Ministros del 24 de junio de 2011. Recuperado de http://www.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf

[28] CONSEJO DE MINISTROS, ESPAÑA. (31 de mayo de 2013). *Aprobada la Estrategia de Seguridad Nacional de 2013.* Nota de prensa. Recuperado de http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/310513Enlace++seguridad.htm

[29] PRESIDENCIA DEL GOBIERNO, ESPAÑA. (1 de diciembre de 2017). Real Decreto 1008/2017, por el que se aprueba la Estrategia de Seguridad Nacional 2017.Un proyecto compartido de todos y para todos Recuperado de http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

Seguridad Nacional el 5 de diciembre de 2013[30].

I.3.- ESTRATEGIA DE SEGURIDAD NACIONAL ESPAÑOLA (ESN)

Es en 2011 cuando se marca en consonancia con la UE, estratégicamente en España, el camino en Seguridad Nacional (con la estrategia de seguridad Nacional 2011) hasta el 2013 que se está consolida con una actualización de la estrategia Nacional amplia y consistente, pero será en diciembre del 2017 cuando se realize la última revisión.

Representa una respuesta a las necesidades en materia de seguridad, considerando como bien lo dice en su presentación "L*a Seguridad Nacional es un servicio público objeto de una Política de Estado, que, bajo la dirección y liderazgo del Presidente del Gobierno, es responsabilidad del Gobierno, implica a todas las Administraciones Públicas y precisa la colaboración de la sociedad en su conjunto". L*a estrategia reconocelos riesgos y vulnerabilidades del estado español, abordándola desde una perspectiva globalizadora, altamente competitivay en contínuo cambio; identifica los entornos estratégicos: *la Unión Europea (UE), el Mediterráneo, América Latina, Estados Unidos y la relación transatlántica, África, Asia, Australia y Rusia. También se tratan la Organización de las Naciones Unidas (ONU), la Organización del Tratado del Atlántico Norte (OTAN) y otros foros multilaterales.*

Asimismo, se vincula a un proyecto común de construcción europea a través del fortalecimiento de mecanismos eficaces de gobernanza económica y financiera y avance hacia la integración política, que es aval de más seguridad y prosperidad para España.

Por otra parte, las estrategias de seguridad en el ámbito del ciberespacio, buscan disminuir "los múltiples riesgos y amenazas que se ciernen sobre las infraestructuras críticas españolas. Su origen puede ser natural o inducido por

[30] CONSEJO DE SEGURIDAD NACIONAL, ESPAÑA. (5 de diciembre de 2013). *Aprobada la Estrategia de Ciberseguridad Nacional de 2013.* Nota de prensa. Recuperado de https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

errores humanos o fallos tecnológicos inesperados"[31].

Sin embargo, son los que se causan deliberadamente, bien por una agresión de carácter físico o por un ataque cibernético, los que revisten mayor peligrosidad, puesto que su móvil y objetivos consisten en ocasionar un daño grave a España y a sus ciudadanos" (RUIZ DÍAZ, 2016). Entre esas infraestructuras críticas tenemos: aeropuertos, centrales nucleares, instalaciones de seguridad y defensa de la Administración del Estado. El análisis de LABORIE[32], la Estrategia de Seguridad Nacional (ESN) dispone de una perspectiva multidisciplinar, que tiene en consideración el nuevo conjunto de amenazas, riesgos y también la concepción estratégica propia de España. Al igual que los países más avanzados, España concibe su Seguridad Nacional por medio del equilibrio ponderado de todos los instrumentos disponibles, tanto públicos como privados. Siguiendo el camino marcado en 2011, la ESN se convierte en un proceso racional conformado por una variedad de acciones cuidadosamente integradas. En cualquier caso, tiene más que ver con el liderazgo que debe guiar su concepción e implementación que con los recursos utilizados. Las Estrategias de Seguridad Nacional no deben ser consideradas un fin en sí mismas. Estos documentos constituyen una referencia de máximo nivel para llevar a cabo el planeamiento estratégico que, como actividad política comprensiva, conlleva decisiones para resolver el problema de seguridad. Por ello, la implantación de una estructura institucional se antoja un elemento esencial para la consecución de la seguridad que España y los españoles necesitan.

Para precisar el análisis de la estrategia de seguridad es pertinente conocer, en términos de cibercriminalidad, las tipologías penales cometidas con las nuevas tecnologías.

Esta clasificación basada en el informe del Anuario estadístico del Ministerio del Interior[33] parte de las tipologías penales descritas en el Convenio sobre

[31] CONSEJO DE MINISTROS, ESPAÑA. (31 de mayo de 2013). Ob., cit., cap. 3, Apartado 12.

[32] LABORIE IGLESIAS, M. (3 de junio de 2014). La estrategia de seguridad nacional (mayo 2013). Instituto Español de Estudios Estratégicos. Madrid: IEEE. Recuperado de http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA34-2013_EstrategiaSeguridadNacional-2013_MLI.pdf

[33] MINISTERIO DEL INTERIOR. ESPAÑA. (2016). Anuario estadístico del Ministerio del Interior 2015. Recuperado de: http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2015.pdf/03be89e1-dd38-47a2-9ce8-ccdd74659741

Cibercriminalidad de Budapest. A estos hechos, se les han unido los delitos contra el honor, las amenazas y coacciones y delitos contra la salud pública, dado el volumen y la importancia que están adquiriendo estos últimos.

Grupos Delictivos	2011	2012	2013	2014	2015
Acceso e interceptación ilícita	1.492	1.701	1.805	1.851	2.386
Interferencia en los datos y en el sistema	228	298	359	440	900
Falsificación informática	1.860	1.625	1.608	1.874	2.361
Fraude informático	21.075	27.231	26.664	32.842	40.864
Delitos sexuales	755	715	768	974	1.233
Contra la propiedad industrial/intelectual	222	144	172	183	167
Contra el honor	1.941	1.891	1.963	2.212	2.131
Amenazas y coacciones	9.839	9.207	9.064	9.559	10.112
Total	**37.412**	**42.812**	**42.403**	**49.935**	**60.154**

***Ilustración 2**: Cibercriminalidad y principales tipologías penales cometidas con las nuevastecnologías.Ministerio del Interior, España (2016, 424).*

La ilustración 2 resume en series temporales, datos entre los años 2011 a 2015, que corresponden a la actividad registrada por las Fuerzas y Cuerpos de Seguridad del Estado Español (Guardia Civil y Policía Nacional) y la Policía Foral de Navarra. También se incluyen datos de los cuerpos de policía local que facilitaron estadísticas al Sistema Estadístico de Criminalidad durante el año 2015. Como se puede apreciar la tendencia al alza es contínua, produciéndose un incremento de más de 10.000 delitos en 2015 con respecto a 2014.

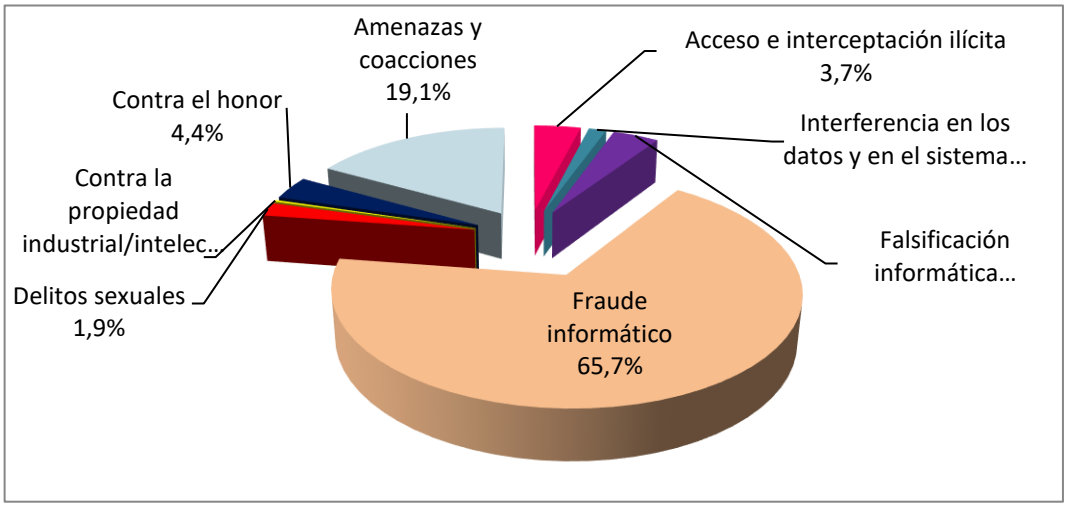


***Ilustración 3**: Porcentaje de tipos penales relacionados con la cibercriminalidad en España (2015). Ministerio del Interior, España (2016, 425).*

En la ilustración 3 se evidencia la distribución porcentual de los ciberdelitos en 2015, de los cuales podemos indicar que el fraude informático (65,7%) es el principal delito cometido en la actualidad, seguido de las amenazas y coacciones (19,1%) y la falsificación informática (3,8%).

Por otra parte, se puede observar en la ilustración 4 el número de hechos conocidos, relacionados con la cibercriminalidad y principales tipologías penales cometidas con las nuevas tecnologías.

Estos hechos relacionados con la cibercriminalidad se han ido incrementando desde 2012 a 2015, hasta alcanzar más de 60.000 casos, de los que casi 20.000 fueron esclarecidos en 2015 a raíz de más de 5.000 detenciones e imputaciones (investigaciones).

***Ilustración 4**: Tabla anuaria de hechos conocidos, esclarecidos e imputaciones. Ministerio del Interior, España (2016, 425).*

Por hechos conocidosse entienden el conjunto de infracciones penales y administrativas que han sido conocidas por las distintas Fuerzas y Cuerpos de Seguridad, bien por medio de denuncia interpuesta o por actuación policial realizada de *motu propio* (labor preventiva o de investigación).

Los hechos esclarecidosse clasifican como tales cuando en el hecho se dan las siguientes circunstancias:

- Detención del autor «*in fraganti*».
- Identificación plena del autor, o de alguno de los autores, sin necesidad de que esté detenido, aunque se encuentre en situación de libertad provisional, huído o muerto.
- Cuando exista una confesión verificada, pruebas sólidas o cuando haya

una combinación de ambos elementos.

- Cuando la investigación revele que, en realidad, no hubo infracción.

El porcentaje de esclarecimiento se obtiene dividiendo el total de hechos esclarecidos por el total de hechos conocidos y multiplicado por 100.

Respecto a la naturaleza de los sujetos responsablesde la comisión de las infracciones penales, se computan las siguientes categorías:

- Imputacióna una persona física o jurídica a la que se atribuya la participación en un hecho penal. No se restringe la libertad.
- Detención: alcanza la lectura de derechos de la persona física, privándola de libertad y poniéndola a disposición judicial, por atribuirle la comisión de una infracción penal.

I.3.1.- Estrategia de Seguridad Nacional 2017

La Estrategia de Seguridad Nacional 2017 fue aprobada por el Gobierno el día 1 de diciembre de 2017 mediante Real Decreto, de acuerdo con lo establecido por la Ley de Seguridad Nacional 36/2015[34]. El Consejo de Seguridad Nacional fue el órgano responsable de su elaboraciónen el que participaron los Ministerios (Asuntos Exteriores y de Cooperación; Justicia; Defensa; Hacienda y Función Pública; Interior; Fomento; Educación, Cultura y Deporte; Empleo y Seguridad Social; Energía, Turismo y Agenda Digital; Agricultura y Pesca, Alimentación y Medio Ambiente; Presidencia y para las Administraciones Territoriales; Economía, Industria y Competitividad; Sanidad, Servicios Sociales e Igualdad), Centro Nacional de Inteligencia y aportaciones de un Comité Asesor independiente (más de 50 expertos: profesores universitarios, analistas de centros de pensamiento, representantes del sector privado y miembros de asociaciones relacionadas con la Seguridad Nacional).

Su coordinación fue realizada por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, en condición de Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional.

[34] Vid. RD 1008/2017. BOE nº 309 de 21 de diciembre de 2017.

La Estrategia actual profundiza en algunos de los conceptos y líneas de acción definidos en 2013 y avanza en la adaptación de dicha Política ante nuevos desarrollos de un entorno de seguridad en cambio constante.

España se enfrenta a una serie de amenazas y desafíos, tanto internos como externos, incluyendo el reto demográfico, su limitada interconexión energética o problemas de cohesión territorial.

Son componentes fundamentales de la Seguridad Nacional la Defensa Nacional, la Seguridad Pública y la Acción Exterior, apoyados por los Servicios de Inteligencia e Información del Estado.

La Ley 36/2015, de 28 de septiembre prevé la revisión de la Estrategia cada cinco años o "cuando lo aconsejen las circunstancias cambiantes del entorno estratégico". La estrategia del 2017 se divide en seis capítulos que abordaremos de forma más extensa a continuación:

Capítulo 1. Una seguridad nacional para la España de hoy:

En este capítulo se describe el perfil de la España actual desde la óptica de los valores constitucionales que propugna, su particular posición geoestratégica, vocación global y los retos derivados del nuevo entorno de seguridad. La seguridad nacional es una política responsabilidad del gobierno y precisa de la colaboración de los ciudadanos.

España es un país europeo, atlántico y mediterráneo, abierto al mundo y protector de sus ciudadanos.

España es un socio fiable en la defensa de los derechos Humanos. Contribuye a la seguridad regional e internacional, de las que a su vez se beneficia. Es un socio fiable presente en la defensa de las mejores causas, como son los Derechos Humanos, la legalidad internacional y el multilateralismo.

España ha desarrollado modelos referenciales en materia de seguridad que ha de seguir actualizando con visión anticipatoria, para actuar frente a amenazas globales que requieren respuestas integrales, coordinadas y cooperativas tanto en

el plano nacional como en el internacional, tanto en la lucha contra el terrorismo como ante el problema creciente de la inmigración.

Es de gran importancia mantener una seguridad económica que convierta nuestro país en un país prospero y seguro además de tener una amplia proyección internacional, estando directamente relacionado con el ámbito energético. España dispone de un gran potencial como nodo energético y puerto de entrada y distribución de recursos en la UE, dado su *mix* energético diversificado por origen y fuentes primarias, su posición geográfica e infraestructuras.

Hay que destacar la necesidad de un control y buen uso de: los espacios marítimos dada la extensa superficie costera de la que dispone el país, sumado al gran porcentaje de población extranjera dentro de nuestras fronteras además de el movimiento que genera nuestro importante sector turístico, generándonos un tránsito de personas y capitales que deben ser regulados y controlados para llevar a buen fin nuestra seguridad Nacional.

La revolución tecnológica es clave para la concepción de la seguridad de España. El éxito de España en el futuro pasa, por tanto, por aprovechar las oportunidades de progreso. Así de manera notable, el desarrollo tecnológico está asociado a una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio.

Otro de los desafíos globales de este tiempo es el **cambio climático**. Un fenómeno que tiene claras repercusiones en el ámbito de la Seguridad Nacional, dado el incremento de la frecuencia y severidad de sequías, inundaciones e incendios, cuyas lineas a seguir vienen recogidas en el Acuerdo de París de reducción de gases contaminantes, firmado en 2015. La conclusión es que España debe fomentar una cultura de Seguridad nacional apoyada con un sistema de educación integrador que ayude a desarrollar una seguridad nacional eficaz donde intervengan las instituciones y los ciudadanos.

Capítulo 2. Dinámicas de transformación de la seguridad global:

En este capítulo abordaremos las transformaciones en el entorno de seguridad global desde la puesta en marcha de la Estrategia de Seguridad Nacional de 2013.

Crisis de variada naturaleza se desencadenan con facilidad y se han convertido en casi una constante de esta era. La distancia entre situaciones de normalidad y crisis es cada vez menor.

En el ámbito geopolítico, dentro de un orden mundial multipolar y cambiante coexisten varios poderes globales y regionales. Están los problemas internos como los independentismos, la hegemonía de EE.UU., el desarrollo potencial de China y Rusia además de contínuos escenarios internacionales que afectan a todo el mundo tanto económica como socialmente, subida del petróleo, movimientos migratorios, los nacionalismos, etc.

Debemos resaltar en este punto la importancia del cambio climático junto con la degradación de los recursos hídricos y la amenaza a la seguridad que éste produce por todos aquellos sucesos que llevan asociados.

Un hecho importante es la manipulación que se produce en la información por parte de agentes externos que ejerce de factor de influencia en la era de la posverdad, con efectos negativos en la cohesión social y la estabilidad política.

La línea de España está comprometida con el orden internacional de legalidad y una gobernanza global, justa, inclusiva y eficaz. España apuesta por la diplomacia preventiva, soluciones pacíficas a los incidentes internacionales y diálogo, incluido el intercultural e interreligioso.

El impacto de las tecnologías es un instrumento de activación económica, crecimiento y progreso, pero también prueba la capacidad de adaptación de las sociedades a los cambios tecnológicos y sobre todo en una disminución alarmante de la Seguridad.

A causa de esta constante exposición al mundo, la conectividad de un mundo en red, internet, inteligencia artificial, ingeniería genética y robotización

están directamente implicados en la seguridad. Hay que diseñar un sistema eficaz de dirección sobre las nuevas tecnologías, englobado en la Seguridad Nacional.

Capítulo 3. España en el mundo: un país con vocación global:

En este capítulo se analizan: la posición geoestratégica de España; los retos y desafíos que, de Seguridad Nacional, sobre distintas regiones del mundo; y las zonas de especial interés.

Aunque hoy en día con la interconectividad desaparecen un porcentaje muy alto de las fronteras, la condición europea y mediterránea de España determina la importancia de estas regiones para su seguridad, estabilidad y prosperidad de España y la UE.

Las fronteras con sus países vecinos, Francia, Marruecos y Portugal estrechan las relaciones estratégicas a nivel de cooperación política, seguridad, defensa e inteligencia. Analicemos las zonas:

América del Norte. España mantiene con EE.UU. y Canadá una relación trasatlántica basada en principios, valores e intereses compartidos

América Latina. España de forma histórica y por lazos socio-políticos está muy unida a estos países, cooperando y actuando de forma conjunta social y económicamente ayudando a Colombia en su proceso de paz y velando por que Venezuela alcance su estabilidad democrática económica y social.

Europa. España desempeña un papel muy importante en la construcción de una UE eficaz, más integrada y legitimada democráticamente; una Unión con capacidad de respuesta, tal y como expone la Estrategia global para la política exterior y de seguridad de la Unión Europea y países candidatos y vecinos, buscando siempre la estabilidad común.

Por otra parte, la OTAN constituye la base de la defensa colectiva de España y Europa. España debe seguir cooperando en materia de seguridad con el Reino Unido y Gibraltar de forma estrecha y amistosa. Además, hay que tener en cuenta la creciente mala relación con Rusia, país de gran influencia en el

consejo de la ONU, debido a su mentalidad expansionista que choca con los límites y valores de la UE

Velar por la paz y proceso de incorporación de los países Balcánicos y Turquía en la UE, como Estados de Derecho, de buen gobierno y respeto a los Derechos Humanos, campos indispensables para su incorporación a la UE.

En definitiva, se necesita de una cooperación estructurada permanente reforzando las líneas en Asuntos de Interior y Justicia de forma cohesionada y con una seguridad conjunta con la OTAN y así de esta forma, los europeos habrán incrementado mucho su seguridad.

Norte de África y Oriente Medio. El Norte de África es una prioridad estratégica para España en relación con el terrorismo Yihadista nacido allí y los movimientos migratorios africanos de seres Humanos, ambos puntos quitan el sueño tanto a España como al conjunto de la UE.

La resolución de los múltiples conflictos en Oriente Medio es uno de los retos más importantes para España y la comunidad internacional.

África subsahariana. En nuestra aproximación a África se requiere de una perspectiva integral de Seguridad, involucrándonos en las políticas de buen gobierno de estos países.

La seguridad cooperativa y las iniciativas de diplomacia preventiva de España y su participación en misiones internacionales (de la ONU y la UE) basadas en buscar la paz y la lucha contra el terrorismo yihadista son parte importante de nuestro cometido.

Asia Pacífico. El peso de influencia de estos países en el panorama mundial está subiendo con mucha rapidez. La inestabilidad que crea Corea del Norte en su zona y la expansión de China en África y sobre todo en América Latina.

Capítulo 4. Amenazas y desafíos para la seguridad nacional:

En este capítulo se identifican:

A) Las principales amenazas y desafíos para la Seguridad Nacional.
B) Los espacios comunes globales más vulnerables.
C) La importancia de las infraestructuras críticas.

Las situaciones, hechos o fenómenos de inestabilidad se podrían decir que, en su mayoría, están interconectadas y en la mayoría de las veces se traspasan fronteras.

El terrorismo yihadista es uno de los principales problemas a los que se enfrenta la comunidad internacional.

En la actualidad es de gran importancia el control de los espacios comunes de no apropiación regulados por el principio de libertad (ciberespacio, el espacio marítimo, terrestre, aéreo y ultraterrestre).

Sobre todo, debemos destacar la exposición de las infraestructuras críticas a las amenazas por el impacto que se podría producir si éstas dejaran de funcionar.

A.1) Principales amenazas para la Seguridad Nacional:

- **1) Conflictos Armados**. Históricamente una de las amenazas más importantes para la Seguridad Nacional. Ahora mismo existe un ambiente de tensión geopolítica, tensión y ruptura del orden internacional. Esto provoca que España deba de mantener una capacidad defensiva (propia, creíble y efectiva). Existen conflictos híbridos llamados así porque combinan operaciones de información, presión económica y financieras con actuaciones militares.

- **2) Terrorismo.** Principalmente el Yihadista que se caracteriza por su ideología radical, globalizada, que en la actualidad azota casi la totalidad del planeta. Ataques realizados por grupos caracterizados por facilidad de

mutación y adaptación a los cambios y estrategias, siendo su principal objetivo el transporte o infraestructuras criticas para conseguir el mayor número de víctimas o inestabilidad quea su vez se convertirá en una estrategia propagandística.

La radicalización, extremismo violento y la captación-adoctrinamiento terrorista son parte de las amenazas de mayor connotación en la actualidad. Todo esto sumado al desarrollo tecnológico multiplica el acceso a recursos disponibles para los grupos terroristas, incrementando su poder de financiación, reclutamiento, adiestramiento y propaganda.

3) Crimen Organizado. Muy desestabilizante y metido de lleno en el uso de las nuevas tecnologías, de carácter trasnacional, elástico y opaco, interrelacionado con el terrorismo, también se vale de la crisis migratoria y de refugiados, y de su vulnerabilidad extrema, para abrir rutas de tráfico humano a Europa. España es canal de acceso a la UE por parte de redes criminales procedentes de África y América.

4) Proliferación de las armas de destrucción masiva. La vertiginosa subida y proliferación de las armas de destrucción masiva (nucleares, químicas, radiológicas y biológicas) y su proyección geográfica a través de misiles, suponen una grave amenaza para la paz y seguridad internacional que afecta directamente a la Seguridad Nacional de todos los países de forma directa o indirecta o bien la posibilidad de que lleguen a manos de los numerosos grupos terroristas. Los países deben llevar un especial control sobre los materiales tóxicos y atómicos de doble uso (tecnológico y militar) para que no puedan ser usados de forma negligente, frenando también el desarrollo militar de países conflictivos en este sentido. La comunidad internacional vela por el respeto del Derecho Internacional Humanitario frente al uso de armas químicas o biológicas contra civiles en guerras por parte de naciones o grupos terroristas.

5) Espionaje. Hablamos de un espionaje tanto de carácter bélico como industrial, que como tantos sectores se ha adaptado especial y formidablemente a las nuevas tecnologías, incluso podemos hablar de espionaje realizado por delincuentes o servicios de inteligencia de algunas naciones que pueden afectar de forma directa

y drástica a nuestra seguridad obligándonos a desarrollar un especializado y exitoso sistema de seguridad cibernética que nos aisle de forma certera o al máximo de todas estas amenazas, en cualquiera de los escenarios posibles.

A.2) Principales desafíos para la Seguridad Nacional:

1) Inestabilidad económica y financiera. Es necesario un enfoque comprehensivo que relacione la dimensión de seguridad con los aspectos económicos cobrando especial importancia la persecución de los grupos terroristas.

2) Vulnerabilidad energética. España es un país energético-dependiente. La prosperidad y estabilidad tanto social como económica del país depende del abastecimiento de energía, pasando por asegurar las instalaciones y los países suministradores.

3) Flujos migratorios irregulares. Europa sufre uno de los sus mayores flujos migratorios. Los inmigrantes pueden suponer parte del bienestar de la zona, aunque de forma desordenada y desorbitada se convierte en un problema y España dentro de la UE se encuentra en un lugar estratégico de entrada donde hay que tomar unas medidas extremas de seguridad por el bienestar general nuestro y del conjunto de la UE.

4) Emergencias y catástrofes. Desafio del mundo actual. Estas no solo afectan a la salud y bienestar de los ciudadanos sino también al patrimonio, medio ambiente y desarrollo económico. Hay cuatro potenciadores en efecto cascada: más población en riesgo, infraestructuras críticas vulnerables, degradación de los ecosistemas e incremento de los fenómenos meteorológicos adversos.

5) Efectos derivados del cambio climático. La subida de las temperaturas actúa sobre la falta de agua y a su vez la falta de recursos naturales lo que desemboca en conflictos armados, España es un país muy vulnerable al cambio climatico por su posición geográfica y su escasez de agua**.**

6) Epidemias y Pandemias. España está expuesta a las corrientes de enfermedades del mundo ya que el mundo está conectado entre sí, y tenemos

alrededor de 75 millones de turistas al año. Es muy importante por un lado la mentalización de los ciudadanos de seguir las normas de seguridad sanitaria y tambien la coordinación y desarrollo de todos los profesionales y organismos implicados buscando siempre la palabra clave “prevención”.

B) Los espacios comunes globales más vulnerables:

Sus características son las siguientes: Apertura geográfica y funcional; Ausencia de soberanía y jurisdicción por parte de los Estados; Facilidad de acceso; y Dificultad de localizar a los actores de las acciones realizadas en estos espacios. Para poder actuar en ellos es clave la cooperación internacional y la asistencia mútua. Son los siguientes:

1) El ciberespacio. Las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. El ciberespacio es un escenario con características propias marcadas por su componente tecnológico, fácil accesibilidad, anonimidad, alta conexión y dinamismo. En los últimos tiempos, las acciones negativas en el ámbito de la ciberseguridad han aumentado notablemente en número, alcance y sofisticación. Tales acciones adquieren creciente relevancia para España, un país altamente interconectado y que ocupa una posición de liderazgo en Europa en materia de implantación de redes digitales.

2) El espacio marítimo. España es una potencia marítima y estratégica. Destaca como punto estratégico el estrecho de Gibraltar. Hay que destacar como puntos calientes: Las rutas marítimas vitales para elcomercio y el transporte; el aprovisionamiento energético y los cables submarinos de información digital. En este espacio aparecen dos principales amenazas: Los actos intencionados y de naturaleza delictiva (piratería, terrorismo, tráficos ilícitos, contra el patrimonio) y los accidentales (producidas por fenómenos naturales).

3) El espacio aéreo y ultraterrestre: Hay que hacer hincapié del control, en los siguientes puntos:

- Violaciones del espacio aéreo.
- Salvaguardar la aviación comercial.
- El uso de drones.

- Salvaguarda y desarrollo de los satélites.
- Competición por el control del espacio ultraterrestre con fines bélicos y comerciales.

C) La importancia de las infraestructuras críticas:

Podemos definir las infraestructuras críticas como aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas.

Estas realizan servicios esenciales para el funcionamiento de tareas sociales, salud, seguridad, bienestar social y económico y sector público (Administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y de comunicaciones, transporte, alimentación y sistema financiero y tributario).

La mayoría de estos servicios son de origen privado por lo que debemos potenciar la colaboración público-privada.

Capitulo 5. Objetivos generales y líneas de acción para la seguridad nacional:

Los objetivos generales orientan la acción del estado en cuanto a seguridad, son comunes para todos los ámbitos (ilustración 6) y los podemos dividir en cinco:

OBJETIVOS SEGURIDAD NACIONAL ESPAÑOLA
OBJETIVO I: Desarrollar el modelo Integral de gestión de crisis.
OBJETIVO II: Promover una cultura de Seguridad Nacional.
OBJETIVO III: Favorecer el buen uso de los espacios comunes globales.
OBJETIVO IV: Impulsar la dimensión de seguridad en el desarrollo tecnológico.
OBJETIVO V: Fortalecer la proyección internacional de España.

***Ilustración 5**: Objetivos Seguridad Nacional Española[35].*

[35]Ibídem., p. 81.

***Ilustración 6**: Amenazas y desafíos para la seguridad Nacional*[36].

Además de estos objetivos generales de la Seguridad Nacional (ilustración 6), vamos a profundizar en los objetivos propios de todos los ámbitos de ésta, concretamente enumerando todas las líneas de acción que son propuestas para dichos ámbitos:

[36] Ibídem., p. 79.

ÁMBITOS DE LA ESTRATEGIA DE SEGURIDAD NACIONAL Y SUS LÍNEAS DE ACCIÓN

1) DEFENSA NACIONAL[37]:

- Mejorar la capacidad de defensa autónoma para ejercer una disuasión efectiva frente a cualquier amenaza exterior.
- Dotar a las Fuerzas Armadas de las capacidades que demanda el actual escenario de seguridad y avanzar decididamente en la convergencia con los objetivos de Defensa establecidos por la OTAN y recomendados por el Parlamento Europeo, como parte de un necesario reparto de responsabilidades, esfuerzos económicos y recursos demandados en todos los planos entre aliados y asegurar la sostenibilidad de una Defensa eficaz a largo plazo.
- Impulsar una estrategia industrial de Defensa que fomente la autonomía en la adquisición de capacidades estratégicas y favorezca la competitividad de la industria española a nivel global.
- Fortalecer la posición de España en el sistema de seguridad internacional, ejerciendo un liderazgo positivo en las organizaciones de seguridad colectiva y coaliciones internacionales de las que forma parte, así como en las relaciones bilaterales.
- Asumir un protagonismo activo en el relanzamiento de la Política Común de Seguridad y Defensa de la UE y continuar siendo un aliado solidario y comprometido con la OTAN, participando asimismo en nuevas formas de cooperación y especialización. A nivel bilateral, ampliar y profundizar el marco de colaboración bilateral con Estados Unidos.
- Contribuir a instaurar un entorno regional de paz y seguridad, prevenir conflictos y contener las amenazas emergentes mediante la proyección de estabilidad y las actividades de seguridad cooperativa, particularmente en las áreas de especial interés para España.
- Potenciar la Diplomacia de Defensa especialmente con países vecinos y aquellos países con los que España comparte intereses y valores, en particular con los países de la orilla sur del Mediterráneo y con América Latina.

2) LUCHA CONTRA EL TERRORISMO[38]:

Prevención:

- Potenciar el desarrollo y total implantación en el territorio español del Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV).
- Reforzar los mecanismos establecidos en materia de lucha contra la financiación del terrorismo.
- Reforzar la contribución de España en la lucha contra el terrorismo a nivel internacional en las organizaciones a las que pertenece, en especial en la OTAN y UE y OTAN y en aquellas iniciativas de las que forma parte.
- Reforzar el testimonio de las víctimas del terrorismo como la mejor vía de contrarrestar la narrativa terrorista. Fomentar el diálogo intercultural e interrreligioso.

Protección:

- Robustecer las capacidades nacionales de lucha contra el terrorismo y la

[37] Ibídem., p. 89.
[38] Ibídem., p. 91.

cooperación y coordinación de esfuerzos contra el terrorismo entre los distintos organismos implicados a nivel nacional.
- Cooperar con los países socios más afectados por el terrorismo y, de forma especialmente estrecha, con la Unión Europea, y adoptar medidas de mejora en el control de fronteras.

Persecución:
- Mejorar las capacidades de investigación e inteligencia, asegurar el desarrollo tecnológico de los servicios de inteligencia e información para hacer frente al uso intensivo de las nuevas tecnologías por parte de los grupos terroristas e impedir el acceso a las capacidades y materiales necesarios para cometer atentados.
- Reforzar los instrumentos legales en la lucha contra el terrorismo, también a nivel internacional, especialmente con el apoyo de la creación de un Tribunal Penal Internacional en materia de terrorismo.

Preparación de la respuesta:
- Robustecer la adopción de las medidas y planes necesarios que aseguren la sinergia y coordinación de todos los organismos con responsabilidad en la materia en caso de atentado terrorista.
- Minimizar las consecuencias y dar apoyo inmediato y permanente a las víctimas de ataques terroristas.
- Consolidar la unidad de los partidos políticos en la lucha contra el terrorismo apoyando el Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo.

3) LUCHA CONTRA EL CRIMEN ORGANIZADO[39]:
- Mantener canales abiertos de formación continua en los métodos y herramientas utilizados por las organizaciones criminales, mediante la colaboración y participación de actores públicos y privados especializados.
- Potenciar la inteligencia estratégica y el intercambio de información como instrumentos de anticipación contra el crimen organizado y reforzar los mecanismos de incautación de los beneficios obtenidos como forma de limitar su capacidad operativa.
- Mejorar la cooperación y coordinación de esfuerzos a nivel internacional para hacer frente a los desafíos del crimen organizado.

4) NO PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA[40]:
- Promover y potenciar el multilateralismo eficaz y el cumplimiento de los compromisos, normativa y organismos que conforman el régimen internacional de no proliferación de armas de destrucción masiva y vectores de lanzamiento.
- Garantizar la seguridad física de los materiales e instalaciones nucleares y radiactivos.
- Luchar contra el tráfico ilícito de materiales y tecnologías relacionadas con las armas de destrucción masiva y sus vectores de lanzamiento. Esto implica reforzar las políticas y practices nacionales e internacionales de control del comercio internacional de materiales de doble uso que pudieran ser utilizados con fines ilícitos, así como impulsar medidas y cooperación internacional para combatir las transferencias ilícitas de conocimiento, tecnología, bienes y equipos relacionados.
- Profundizar y promover la cooperación internacional para fortalecer la seguridad de la cadena logística internacional y el control fronterizo para la detección de

[39]Ibídem., p. 93.
[40]Ibídem., p. 95.

posibles tráficos ilícitos de estos materiales, mejorando la identificación e información sobre transacciones sospechosas.
- Fortalecer las capacidades nacionales en el área de la no proliferación mediante la aplicación de la normativa internacional y el desarrollo y actualización de la normativa nacional.
- Profundizar en los mecanismos para la prevención, detección y control de los flujos financieros relacionados con la proliferación y apoyo a los esfuerzos internacionales en este campo, en línea con las resoluciones del Consejo de Seguridad de Naciones Unidas y los Reglamentos de la UE.
- Colaboración y desarrollo de los controles aduaneros en el ámbito de análisis de riesgos.
- Promover programas de divulgación eficaces para informar y concienciar a la sociedad civil: universidades, centros de investigación e industria respecto de las responsabilidades y consecuencias, tanto morales como penales, del desvío de materiales de doble uso que pudieran ser utilizados con fines ilícitos.

5) CONTRAINTELIGENCIA[41]:
- Reforzar las capacidades de los órganos nacionales de inteligencia, con objeto de garantizar la disposición de los medios humanos y técnicos necesarios para contrarrestar eficazmente esta amenaza.
- Potenciar la protección de la información clasificada.
- Incrementar la cooperación internacional en materia de contrainteligencia, tanto en el ámbito bilateral como en los organismos multinacionales de seguridad y defensa de los que España forma parte, para proporcionar una respuesta integral en defensa de los intereses nacionales.
- Intensificar las actividades de contrainteligencia en el ciberespacio.

6) CIBERSEGURIDAD[42]:
- Reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta e investigación frente a las ciberamenazas, así como potenciar la coordinación en los niveles técnico y estratégico del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad.
- Reforzar, impulsar y promover los mecanismos normativos, organizativos y técnicos, así como la aplicación de medidas, servicios, buenas prácticas y planes de continuidad para la protección, seguridad y resiliencia en (1) el Sector Público, (2) los sectores estratégicos (especialmente en las infraestructuras críticas y servicios esenciales), (3) el sector empresarial y (4) la ciudadanía, de manera que se garantice un entorno digital seguro y fiable.
- Reforzar y mejorar las estructuras de cooperación público-público y pública-privada nacionales en materia de ciberseguridad Alcanzar las capacidades tecnológicas necesarias mediante el impulso de la industria Española de ciberseguridad, promoviendo un entorno que favorezca la investigación, el desarrollo y la innovación así como la participación del mundo académico.
- Promover el alcance y mantenimiento de los conocimientos, habilidades, experiencia, así como capacidades tecnológicas y profesionales que necesita España para sustentar los objetivos de la ciberseguridad.
- Contribuir a la seguridad del ciberespacio, en al ámbito de la Unión Europea e internacional, en defensa de los intereses nacionales, fomentando la cooperación y el cumplimiento del Derecho internacional.

[41] Ibídem., p. 97.
[42] Ibídem., p. 99.

7) SEGURIDAD MARÍTIMA[43]:

- Promover un enfoque integral que potencie la actuación coordinada y cooperativa de las diferentes Administraciones en la resolución de problemas que afectan a la seguridad marítima.
- Adoptar medidas para fortalecer la capacidad de actuación del Estado en la mar y en su litoral en un empleo óptimo de máximo aprovechamiento de los recursos.
- Fomentar la colaboración con el sector privado.
- Fomentar la cooperación internacional, en particular a través de la aplicación de las iniciativas de la Organización Marítima Internacional, la Estrategia de Seguridad Marítima de la UE, y la Estrategia Marítima de la OTAN.
- Mejorar la ciberseguridad en el ámbito marítimo.

8) SEGURIDD DEL ESPACIO AÉREO Y ULTRATERRESTRE[44]:

- Fomentar una actuación coordinada de todas las Administraciones Públicas y departamentos con competencias en el espacio aéreo y ultraterrestre que permita establecer sinergias y abordar soluciones transversales.
- Fortalecer las capacidades de los organismos e instituciones nacionales, tanto públicos como privados, con competencias en estos ámbitos, para hacer frente a las diversas amenazas y desafíos propios del espacio aéreo y ultraterrestre.
- Perseverar en el análisis de riesgos y evaluación de medidas contra ciberataques, actos terroristas o delictivos u otros conflictos que afecten a las instalaciones aeroportuarias, o al transporte aéreo dentro o fuera del espacio aéreo español.
- Impulsar un desarrollo normativo del uso civil de aeronaves pilotadas remotamente que garantice el necesario equilibrio entre la seguridad de las personas, instalaciones y demás usuarios del espacio aéreo, y el desarrollo tecnológico y económico de un sector pujante de la economía española.
- Apoyar el papel de España en el ámbito internacional dentro del marco de compromisos y responsabilidades asumidos en materia de seguridad aérea y ultraterrestre.

9) PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS[45]:

- Avanzar en el cumplimiento de la normativa sobre protección de infraestructuras críticas y en el proceso de planificación escalonada previsto en dicha normativa.
- Potenciar la seguridad integral de las infraestructuras críticas a través de todas aquellas actuaciones de planificación, prevención, reacción, mitigación del daño y restitución del servicio que resulten oportunas.
- Incrementar la capacidad y resiliencia de los sistemas asociados a las infraestructuras críticas, impulsando la implantación de programas de gestión de riesgos, de acuerdo con las prioridades establecidas en el Plan Nacional de Protección de las Infraestructuras Críticas.
- Promover la coordinación en materia de protección de infraestructuras críticas, lucha contra el terrorismo y ciberseguridad ente todas las organizaciones responsables, mejorando las capacidades de todas ellas.
- Estimular la cooperación público-público y público-privada en el marco del Sistema Nacional de Protección de las Infraestructura Criticas, incentivando el intercambio de información con el establecimiento de procedimientos y canales seguros y confiables.
- Favorecer la innovación en seguridad, equipando progresivamente a las

[43]Ibídem., p. 101.
[44]Ibídem., p. 103.
[45]Ibídem., p. 105.

infraestructuras críticas de sistemas y componentes de seguridad desde el diseño, y apostando por la tecnología y el desarrollo I+D+i español.
- Impulsar la colaboración internacional y avanzar en el desarrollo de las estructuras y sistemas de intercambio de información y alerta temprana entre países, y en particular entre los Estados miembros de la UE..

10) SEGURIDAD ECONÓMICA Y FINANCIERA[46]:

- Profundizar en el desarrollo de órganos, organismos, recursos y procedimientos (Sistema de Seguridad Económica) que fomenten la coordinación, colaboración, cooperación e intercambio de información entre las distintas Administraciones Públicas con competencias en materia de seguridad y en el ámbito económico-financiero, así como con el sector privado, con el fin de responder eficazmente a los desafíos que limitan el desarrollo y la competitividad de la economía española y amenazan la Seguridad Nacional.
- Reforzar el uso eficiente y la generación de información e inteligencia, tecnologías, legislación, formación y alianzas estratégicas para salvaguardar y promover los intereses económicos nacionales y fomentar una responsabilidad compartida sobre las amenazas y desafíos para la continuidad de la actividad económica.
- Fomentar la efectividad e independencia de los órganos administrativos relacionados con la seguridad económica y la regulación.
- Continuar el esfuerzo de mejora del intercambio de información internacional como herramienta para la prevención y la lucha contra el fraude fiscal.
- Avanzar en la Unión Económica y Monetaria como fuente de confianza, crecimiento y prosperidad.
- Impulsar un Mercado Único Europeo y la libertad de comercio internacional, especialmente en el marco de las instituciones y foros internacionales y mediante la cooperación, asumiendo una posición proactiva que garantice la seguridad y prosperidad de la actividad económica nacional.
- Promover una gobernanza internacional justa que promueva la transparencia y luche contra la corrupción, impulse un crecimiento inclusivo y equitativo y favorezca una mejor efectividad y representatividad en las instituciones reguladoras.
- Favorecer la innovación de la economía, acompañada de una regulación acorde al ritmo de los cambios tecnológicos, que permita incrementar la diferenciación de los bienes y servicios ofrecidos por las empresas españolas.

11) SEGURIDAD ENERGÉTICA[47]:

- Contribuir al fortalecimiento de la seguridad energética en el conjunto de la UE.
- Asegurar la diversificación del mix energético nacional, proporcionando una adecuada representación de las fuentes energéticas y fomentando el uso de fuentes autóctonas que disminuyan la dependencia exterior.
- Garantizar la seguridad del abastecimiento y del suministro con objeto de asegurar el acceso a los recursos necesarios en todo momento y del transporte, tanto terrestre como marítimo, para alcanzar la provisión de los recursos necesarios en tiempo oportuno.
- Impulsar la transición energética hacia un modelo basado en la eficiencia e integración de las variables ambientales en los procesos de toma de decisión.
- Promover la seguridad de las infraestructuras energéticas frente a catástrofes de origen natural, accidentes de origen técnico, errores humanos y amenazas

[46] Ibídem., p. 107.
[47] Ibídem., p. 109.

cibernéticas.
- Reforzar la seguridad integral de las infraestructuras del sector energético y, en particular, de aquellas consideradas críticas, frente a las amenazas físicas y cibernéticas que puedan ponerlas en grave riesgo.

12) ORDENACIÓN DE FLUJOS MIGRATORIOS[48]:
- Fomentar la colaboración entre las Administraciones Públicas y, en su caso, con las organizaciones no gubernamentales y el sector privado, con el objetivo de prevenir los riesgos asociados a la inmigración irregular.
- Vigilar y controlar los accesos a las fronteras exteriores españolas en el marco del Sistema Integrado de Gestión de las Fronteras Exteriores de la UE.
- Defender la legalidad y preservar de la seguridad ciudadana, mediante la lucha contra la discriminación y la promoción de la integración social y, en concreto:
    - Adaptar de forma progresiva el modelo de integración en sus diferentes ámbitos de proyección.
    - Luchar contra la discriminación y garantizar el principio de igualdad, con especial atención a los colectivos más vulnerables.
    - Proporcionar una adecuada acogida, asistencia y protección de los solicitantes y beneficiarios de protección internacional, en cumplimiento de la normativa aplicable.
- Promover la conformación de una política migratoria y de asilo común en la UE y dar cumplimiento adecuado a los compromisos asumidos.
- Cooperar con los países de origen y tránsito migratorio para favorecer su desarrollo, fomenter vías de inmigración legal, prevenir en origen la inmigración irregular y luchar contra las redes de inmigración y el tráfico ilícito de personas..

13) PROTECCIÓN ANTE EMERGENCIAS Y CATÁSTROFES[49]:
- Elaborar, aprobar e implantar de forma cooperativa en todas las Administraciones competentes la Estrategia del Sistema Nacional de Protección Civil, tras su aprobación por el Consejo de Seguridad Nacional.
- Completar el marco jurídico de la protección ante emergencias y catástrofes, desarrollando reglamentariamente la Ley 17/2015.
- Fomentar la colaboración público-privada, especialmente en materia de prevención.
- Fortalecer la integración de capacidades de todo el Sistema Nacional de Protección Civil incrementando la cooperación y coordinación entre todas las Administraciones públicas competentes, con actuaciones concretas:
    - Constituir e implantar la Red de Alerta Nacional de Protección Civil para mejorar la prevención, con un enfoque integrado y multirriesgo.
    - Mantener directorios de capacidades.
    - Diseñar en común acciones de asistencia integral a las víctimas.
    - Establecer protocolos de gestión y comunicación a nivel nacional e internacional, en coordinación con la UE y otros organismos internacionales.
- Promover la coordinación y cooperación internacional en materia de Protección Civil, con especial atención al Mecanismo de Protección Civil de la UE y la Estrategia Internacional de Reducción del Riesgo de Desastres de la ONU, así como, de forma bilateral, con terceros países.

[48]Ibídem., p. 111.
[49]Ibídem., p. 113.

14) SEGURIDAD FRENTE A PANDEMIAS Y EPIDEMIAS[50]:

- Adaptar servicios de salud pública del Estado y Comunidades Autónomas para asegurar una adecuada capacidad de respuesta operativa.
- En lo que se refiere a la mejora de las capacidades y mecanismos de actuación:
  - Revisar y actualizar periódicamente los planes de preparación y respuesta existentes ante riesgos específicos.
  - Promover el desarrollo de un plan nacional genérico de preparación y respuesta ante riesgos biológicos con una aproximación multisectorial.
  - Establecer los mecanismos necesarios para la coordinación de las Fuerzas Armadas, Fuerzas y Cuerpos de Seguridad del Estado, los responsables judiciales y las autoridades de salud pública para dar una respuesta eficaz ante ataques intencionados con agentes infecciosos.
  - Adaptar la Red de hospitales de tratamiento de casos confirmados de Ébola para responder ante cualquier enfermedad infecciosa de alto riesgo.
  - Ampliar y mantener los sistemas de vigilancia y control de introducción de vectores exóticos en puntos de entrada y de vectores autóctonos, además de extender el Plan Nacional de Preparación y Respuesta Frente a Enfermedades Transmitidas por Vectores a todos los vectores de interés.
  - Desarrollar y mejorar entre los departamentos ministeriales involucrados los protocolos para evitar la entrada en el país de animales o mercancías que puedan contener patógenos de riesgo, así como para garantizar la atención adecuada a personas que accedan al país con enfermedades infecciosas de alto riesgo.
  - Reforzar las capacidades de respuesta de equipos de intervención de sanidad exterior ante incidentes sanitarios en fronteras.
  - Adoptar protocolos de gestión y comunicación de situaciones de crisis alimentarias en coordinación con la UE y otros organismos internacionales de referencia.
- Impulsar la coordinación internacional para el intercambio de información y el conocimiento sobre la gestión y tratamiento de nuevas enfermedades.
- Desarrollar los Equipos Técnicos Españoles de Ayuda y Respuesta en Emergencias (START) y
- favorecer su participación en misiones internacionales..

15) PROTECCIÓN DEL MEDIO AMBIENTE[51]:

- Profundizar en el seno de la UE en el cumplimiento de los compromisos asumidos para la preservación del medio ambiente, la biodiversidad, la prevención de la inseguridad hídrica y, muy especialmente, la lucha contra el cambio climático avanzando en la cooperación internacional.
- Potenciar la coordinación entre los distintos componentes del sector público, de manera que se favorezca la creación de las sinergias necesarias entre aquellos con responsabilidad en la conservación y mejora del medio ambiente. Ello se hará asimismo extensible a la colaboración público-privada.
- Fortalecer y ampliar las capacidades, tanto genéricas como especializadas, orientadas a la lucha contra las agresiones al medio ambiente que constituyen una verdadera amenaza para el entorno natural y la calidad de vida de las personas. A tal efecto se desarrollarán acciones orientadas a:
  - Integrar la variable de adaptación y mitigación del cambio climático y disminución de la contaminación atmosférica y acústica en todas las

[50]Ibídem., p. 115.
[51]Ibídem., p. 117.

planificaciones sectoriales, con la finalidad de apostar por las actuaciones menos contaminantes y que permitan una mejor adaptación a los impactos, tanto físicos como económicos, del cambio climático.
- Mejorar las capacidades de prevención y respuesta a la contaminación del medio marino.
- Apoyar el uso de tecnologías menos contaminantes e impulsar nuevas energías alternativas que aminoren el impacto ambiental en todos los sectores de actividad económica.
- Desarrollar iniciativas de carácter preventivo, de respuesta y de recuperación de daños en materia de incendios forestales y promover sumideros forestales.
- Mantener los esfuerzos en materia de planificación para la adecuada gestión de la escasez hídrica, con especial atención a los riesgos de inundación y sequía.

Capitulo 6. Sistema de Seguridad Nacional:

Se trata de implantar un Sistema de Seguridad Nacional dirigido por el Consejo de Seguridad Nacional bajo el mando del Presidente del Gobierno y donde participa tanto el estado como los ciudadanos.

Cabe destacar la asistencia que recibe el CSN por parte del comité de situación que trata de coordinar las actuaciones entre las administraciones públicas para poder responder con efectividad a las situaciones de crisis.

En el ámbito legislativo, España cuenta con la comisión mixta Congreso-Senado de Seguridad Nacional, de donde nace la Ley 36/2015 que fue aprobada bajo notable consenso.

Destacar las nuevas iniciativas que el gobierno desarrollará en base a los objetivos generales de esta nueva ESN.

1) Complementar el modelo de gestión de crisis de alcance Nacional (integral, preventivo, anticipatorio, resilente y eficaz).
2) Aprobar el plan integral de cultura de SN (inclusivo, participativo y colaborativo).
3) Diseñar la posición estratégica nacional respecto al gobierno y uso de los espacios comunes globales.
4) Impulsar el desarrollo tecnológico seguro. (Será el punto de contacto único en el ámbito de redes e información del CSN con las autoridades de toda la UE).

I.3.2.- Ciberseguridad

El objetivo es "garantizar un uso seguro de las redes y los sistemas de informacióny comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable"[52].

En este aspecto, que es punto fundamental de nuestra investigación es pertinente acotar en palabras de SUBIJANA ZUNZUNEGUI (2008, p. 182), "una primera norma significativa en materia de ciberterrorismo es la referida a la extensión de la potestad jurisdiccional de los órganos judiciales que conforman el Poder Judicial de España. La función jurisdiccional, en cuanto ejercicio de uno de los poderes del Estado (el de juzgar y hacer ejecutar lo juzgado), requiere normalmente, cuando se trata del ejercicio del *ius puniendi*, de la existencia de alguna conexión entre la infracción y el Estado. Este nexo puede ser el territorio (principio de territorialidad), la nacionalidad del infractor o la víctima (principio de personalidad) o la protección de los intereses esenciales del Estado (principio de protección de intereses). Una excepción a esta exigencia común de nexo entre el Estado y el delito constituye el principio de jurisdicción universal que permite al Estado perseguir y juzgar a las personas por los crímenes cometidos fuera de su territorio, cualquiera que sea la nacionalidad de los autores o víctimas. Pues bien, conforme a lo establecido en el artículo 23.4 b LOPJ, el ciberterrorismo está sujeto al principio de justicia universal. Por lo tanto, la jurisdicción española puede proceder a su enjuiciamiento cualquiera que sea el lugar en el que se cometa el delito o la nacionalidad de sus autores o víctimas".

Por otra parte, la Unión Europea ha realizado diversos esfuerzos relacionados con la Ciberdefensa[53]:

- El primero de ellos focalizado en la Protección de Infraestructuras Críticas, encuadrando dentro de ellas a las TIC (como infraestructuras en si, por un lado, y como soporte para el funcionamiento de otras

52 Ibídem., p. 100.
53 PASTOR ACOSTA, et al. (2009). Ob., cit.

infraestructuras críticas por otro). Dentro de este ámbito, los esfuerzos realizados han sido encaminados a la puesta en marcha del Programa Europeo para la Protección de las Infraestructuras Críticas (PEPIC) y una Red de Alerta en relación con las Infraestructuras Críticas (CIWIN).

- El segundo foco, más centrado en la Ciberdefensa, en el que los esfuerzos se pueden dividir en dos vertientes:

- Una primera área relacionada con la mejora de la protección de los sistemas de información. La Comunicación de la Comisión de 31 de mayo de 2006.

  "Una estrategia para una sociedad de la información segura - Diálogo, asociación y potenciación". La Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, de 6 de junio de 2001, "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo".

- La segunda área relacionada con la "Lucha contra los delitos" que abarca la vertiente legislativa y de persecución, en donde los aspectos más destacados son todos aquellos relacionados con la "lucha contra el Cibercrimen", como por ejemplo la Decisión Marco 2005/222 sobre "ataques contra los sistemas de información".

La primera área de la ciberdefensa se empezó a desarrollar tras los atentados de Madrid, en marzo de 2004. La Comisión Europea adoptó la Comunicación sobre protección de las infraestructuras críticas sobre la que España, en mayo de 2007, aprobó el Plan Nacional de Protección de las Infraestructuras Críticas y creó posteriormente el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)[54].

En cuanto a los esfuerzos realizados por el país, específicamente en Ciberdefensa, los más destacados son la labor realizada por el CCN para incrementar la Seguridad de la Información en la Administración pública, y la

[54] Antes denominado Centro Nacional de Protección de Infraestructuras Críticas, vid. Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Vid. http://www.cnpic.es/

participación del Ministerio de Defensa como miembro del Centro de Excelencia de Ciberdefensa Cooperativa (CCD COE) de la OTAN, ubicado en Estonia.

Finalmente, hay que notar que España es uno de los pocos países de la UE que a finales de 2008 todavía no habían informado a la misma sobre el grado de aplicación de la normativa comunitaria, aprobada en el año 2005, sobre ataques contra los sistemas de información (PASTOR ACOSTA, et al, 2009).

Respecto a la Ciberdefensa, resaltar que el Ciberespacio se ha convertido en un nuevo "campo de batalla" (a nivel civil y militar). Por ello, está ganando peso en la actualidad a pasos agigantados, y tendrá una mayor relevancia en el futuro cercano para todas las naciones.

Los Ciberataques se están convirtiendo en un arma "barata", "silenciosa" y "fácil de enmascarar" para cualquier organización con intereses hostiles, y pueden tener efectos desastrosos en aquellos países u organizaciones que los sufren. Es importante tener en cuenta que la Ciberdefensa no debe ser una actividad aislada en sí misma, sino que debería estar incluida, o contemplarse desde las siguientes perspectivas:

- Dentro de las Estrategias de Seguridad Nacional.
- Dentro de la Protección de Infraestructuras Críticas.
- Dentro de la Lucha contra Organizaciones Terroristas y Criminales.

La Ciberseguridad es el conjunto de medidas, de carácter técnico o no, que se encargan de proteger tanto la parte concerniente a las infraestructuras globales, que facilitan la circulación de la información (lo que podríamos definir como el entorno macro del ciberespacio) como los dispositivos que procesan, transmiten o almacenan la información que circula por el nivel macro (lo que podríamos definir como nivel meso) y finalmente el nivel micro, compuesto por el software y los datos intangibles generados por el mismo.

Los tres niveles del ciberespacio son vulnerables (no sólo por ataques intencionados, ya que la vulnerabilidad puede ser debida a desastres naturales) por lo que es necesario establecer medidas de protección en todos los casos. Cada uno de ellos debe tener su propia estrategia de seguridad dependiendo de la criticidad de las vulnerabilidades y la gravedad de sus consecuencias.

Queda justificado que el uso de Internet con fines terroristas como instrumento y/o medio para la comisión de sus actos es una realidad; Internet y las infraestructuras TIC como objetivo terrorista, es una hipótesis que cada vez toma más fuerza como una amenaza emergente.

El ciberespacio, plantea una serie de vulnerabilidades, que en el caso de las infraestructuras críticas son especialmente importantes. Los peligros principales son: La amplia interconexión entre las mismas, que genera múltiples dependencias entre ellas y la posibilidad de efectos en cascada; La posibilidad de convertirse en objetivos de ataque directo, o dentro de una acción concertada con un atentado convencional; La amplificación de los efectos psicológicos en la población que supondría un ataque de estas características por su repercusión en infraestructuras vitales para la población (RUIZ DÍAZ, 2016).

Para responder con la mayor rapidez posible a las ciberamenazas y facilitar información preventiva sobre las mismas, se han creado distintos CERT (*Computer Emergency Response Team)* dependientes de organismos como el CCN (Centro Criptológico Nacional), CERTSI (CERT de Seguridad e Industria), INCIBE (Instituto Nacional de Ciberseguridad) o REDIRIS (Red Española para la Interconexión de Recursos informáticos) que gestionan e investigan los posibles incidentes que afectan a la seguridad del ciberespacio y facilitan herramientas de eliminación de virus y consejos de seguridad para evitar vulnerabilidades de los equipos informáticos.

I.4.- ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

La era de la Tecnología, Información y Comunicación se encuentra dentro de nuestra vida cotidiana y nuestropaís. Este nuevo hábitat desarrolla el intercambio de información y las comunicaciones, aunque de forma negativa aumenta de forma exponencial la integridad y éxito de la Seguridad Nacional.

Dependemos del ciberespacio; ello nos obliga a fomentar y comprometernos con todos los medios necesarios y capacidades para mantener con exito nuestra ciberseguridad.

Nuestra Estrategia de Ciberseguridad Nacional es un modelo basado en la implicación, coordinación y armonización de todos los componentes humanos, técnicos y recursos del Estado. Es muy importante la participación de la ciudadanía y empresas privadas, así como su mútua colaboración y cooperación, aunque dado el carácter transnacional de la ciberseguridad, es absolutamente necesaria la cooperación con la Unión Europea, OTAN y otros organismos de ámbito internacional para alcanzar el éxito en nuestra ciberseguridad.

El objetivo primordial de la estrategia de ciberseguridad es el de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas. La estrategia consta de 5 capítulos que se abordarán a continuación:

Primer capítulo: <u>El ciberespacio y su ciberseguridad</u>:

Queda más que patente la fuerte dependencia de la sociedad actual de las TIC y además ésta crece de forma continuada. Las TIC han conseguido tal rapidez y facilidad de intercambio de información y comunicación que han eliminado las barreras de distancia y tiempo.

El medio que facilita este tipo de acciones de comunicación es el ciberespacio que a su vez da cobijo a los ciberataques. Los ciberataques se caracterizan por el bajo coste, ubicuidad y fácil ejecución, efectividad e impacto y reducido riesgo para el atacante (ilustración 7).

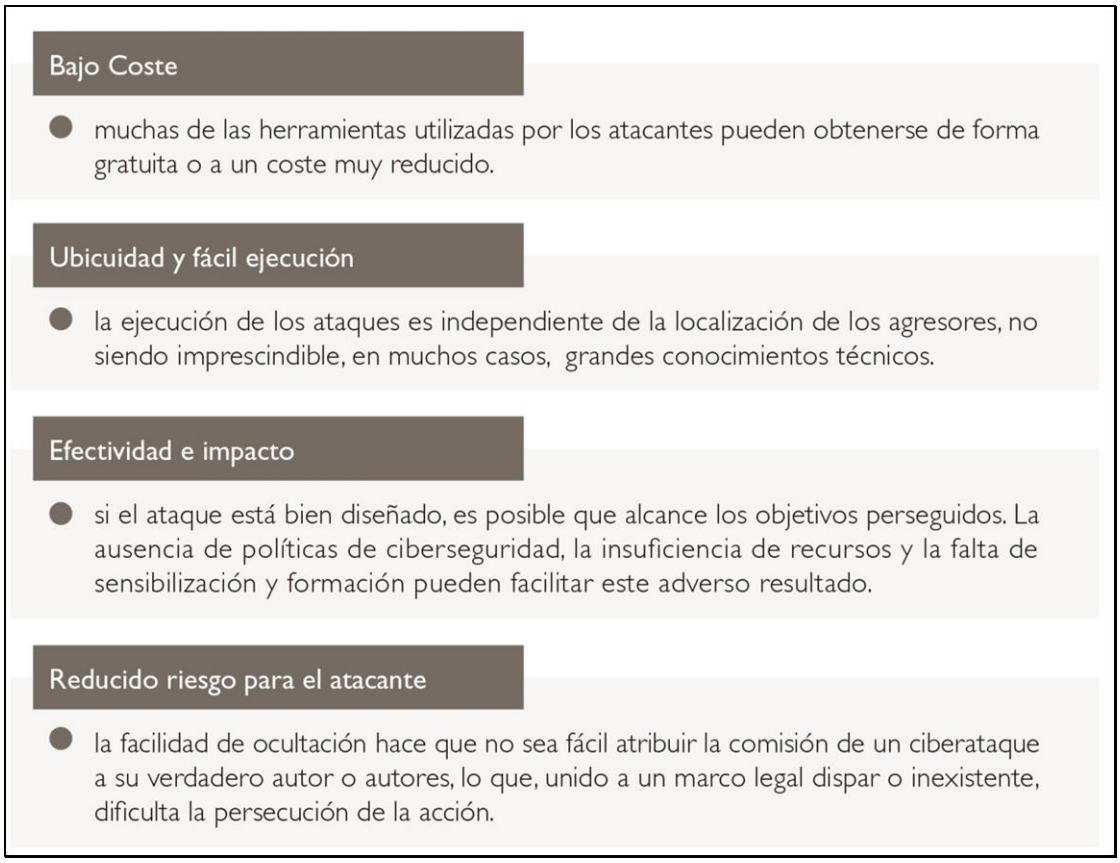


***Ilustración 7**: Características de los ciberataques[55].*

Es tal la cantidad y poder de destrucción de los ciberataques que se ha convertido "la ciberseguridad en una necesidad de nuestra sociedad y modelo económico"[56] hasta tal punto que la estabilidad y prosperidad de España dependen de ella. En el ciberespacio tienen cabida los riesgos y amenazas a la seguridad (ilustración 8).

[55] CONSEJO DE SEGURIDAD NACIONAL, ESPAÑA. (5 de diciembre de 2013). Ob., cit., p. 10.
[56] Ibídem., p. 10.

***Ilustración 8**: Riesgos y amenazas a la seguridad nacional*[57].

Segundo capítulo: Propósito y principios rectores de la ciberseguridad en España:

El propósito general de la Estrategia de Ciberseguriad Nacional promovida por el Consejo de Seguridad Nacional es fijar las directrices del uso del ciberespacio. Su principal objetivo es el de estimular una utilización libre, segura y eficiente del ciberespacio por parte de todos los ciudadanos, basándose en los principios generales de la soberanía estatal, las ideas generales contenidas en la Estrategia de ciberseguridad de la UE y en la estricta observancia del Convenio Europeo de Derechos Humanos, la Carta de los Derechos Fundamentales de la UE, y la protección de los derechos fundamentales, libertad de expresión, datos personales y privacidad (ilustración 9).

[57] Ibídem., p. 11.

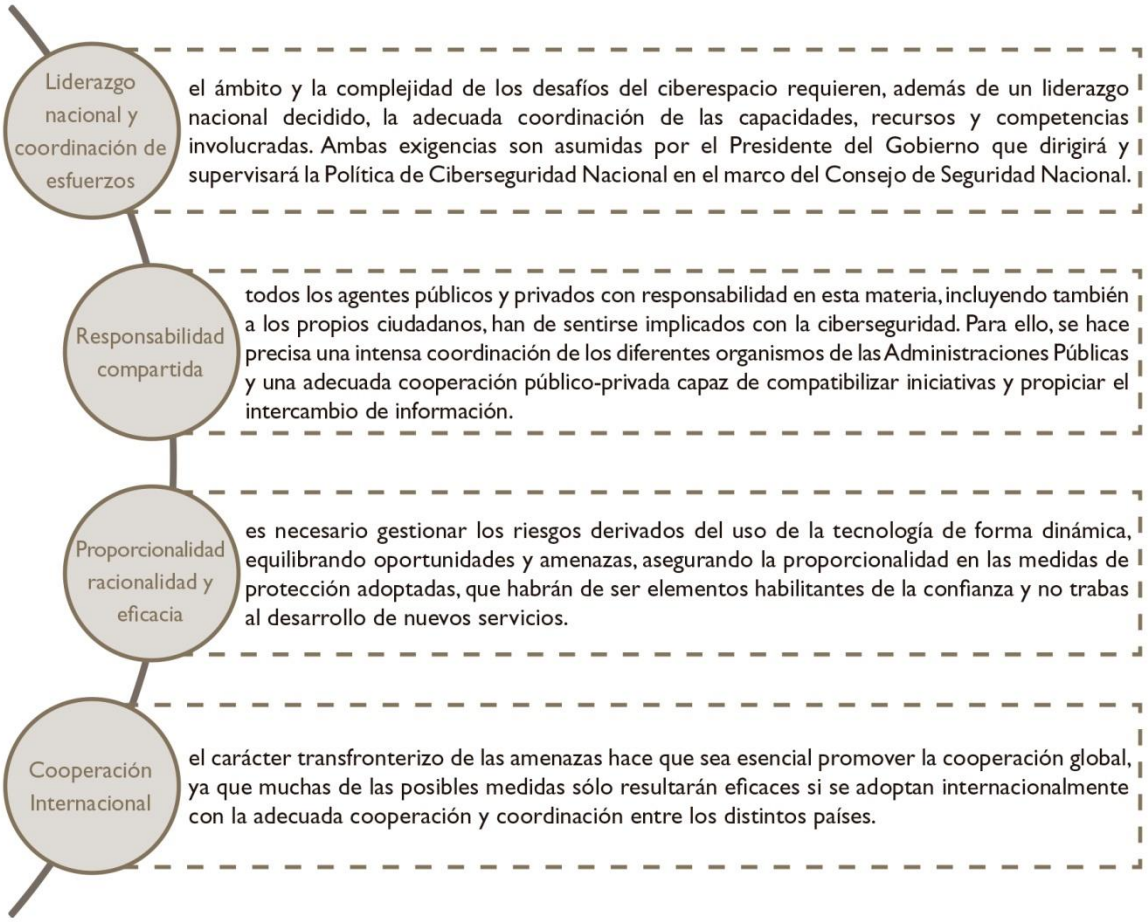


***Ilustración 9**: Principios rectores*[58].

Tercer capítulo: Objetivos de la ciberseguridad:

Podríamos hablar de un objetivo global y seis objetivos específicos todos ellos promovidos por una política de ciberseguridad nacional y resumidos en la ilustración 10.

[58] Ibídem., p. 16.

OBJETIVOS DE LA CIBERSEGURIDAD ESPAÑOLA

OBJETIVO I: Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia. "Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública."
OBJETIVO II: Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular. "Se debe asegurar la Protección del Patrimonio Tecnológico de España".
OBJETIVO III: Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio. "Es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales".
OBJETIVO IV: Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio. "Las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan".
OBJETIVO V: Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad. "Se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva.
OBJETIVO VI: Contribuir a la mejora de la ciberseguridad en el ámbito internacional. "Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa"

***Ilustración 10**: Objetivos de la estrategia de ciberseguridad española[59].*

Objetivo Global: Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.

"Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia".

[59] PONS GAMÓN, V. (2018). Ob., cit.

Cuarto capítulo: Líneas de acción:

Es imprescindible para alcanzar sus objetivos que la estrategia de ciberseguridad establezca ocho líneas de acción resumidas en la siguiente tabla (ilustración 11):

LÍNEA DE ACCIÓN		CONTENIDO
1	**Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas**	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas**	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas**	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	**Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	**Seguridad y resiliencia de las TIC del sector privado**	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	**Conocimientos, Competencias e I+D+i**	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
7	**Cultura de ciberseguridad**	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	**Compromiso internacional**	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

***Ilustración 11**: Líneas de acción de la estrategia de ciberseguridad española[60].*

[60] Ibídem., p. 40.

Capítulo 5: La ciberseguridad en el Sistema de Seguridad Nacional:

La ciberseguridad es un conglomerado de organizar y llevar a cabo con éxito los objetivos, líneas de acción y aplicación de legislación vigente con respeto a los derechos internacionales (ilustración 12).

***Ilustración 12**: Estructura orgánica de la ciberseguridad nacional*[61].

El Sistema de Ciberseguridad Nacional se organiza en tres estamentos de consejo y dirección:

1) Consejo de Seguridad Nacional: Es una comisión delegada del gobierno para la seguridad nacional a modo de *staff* del presidente del gobierno para la dirección de la política de seguridad Nacional.

El Consejo de Seguridad Nacional, en su reunión de 1 de diciembre de 2017, ha adoptado un Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad.

Esta orden se aprueba como actualización de la estrategia nacional de ciberseguridad del 2013.

[61] Ibídem., p. 43.

A continuación, puede verse la ilustración 13 donde se explica la estructura de este acuerdo de enero 2018 para regular el Consejo Nacional de Ciberseguridad.

ACUERDO POR EL QUE SE REGULA EL CONSEJO NACIONAL DE CIBERSEGURIDAD 2018

Primero, Objeto: El presente Acuerdo tiene por objeto establecer el marco regulador del Consejo Nacional de Ciberseguridad (en adelante el Consejo) de conformidad con lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Segundo. Naturaleza jurídica: El Consejo es un órgano de apoyo del Consejo de Seguridad Nacional de los previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que corresponde ejercer las funciones asignadas por aquel en el ámbito de la ciberseguridad y en el marco del Sistema de Seguridad Nacional, según se concretan en este Acuerdo.

Tercero. Régimen jurídico aplicable: El Consejo se rige por lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, por el presente Acuerdo y por sus Normas de régimen interno y de funcionamiento.

Cuarto. Funciones específicas: El Consejo ejercerá las siguientes funciones:

1. Proponer al Consejo las directrices en materia de planificación y coordinación de la política de Seguridad Nacional relacionadas con la ciberseguridad.
2. Reforzar el adecuado funcionamiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad, cuya supervisión y coordinación corresponde al Consejo.
3. Apoyar al Consejo en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y poder proponer su revisión, en lo relacionado con la ciberseguridad.
4. Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional y los instrumentos de desarrollo aprobados, para ulterior informe al Consejo de Seguridad Nacional, con propuestas para una posible revisión de la existente o aprobación de una nueva estrategia sectorial.
5. Contribuir a la elaboración de propuestas normativas para el fortalecimiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad.
6. Apoyar la toma de decisiones del Consejo de Seguridad Nacional en las materias propias del ámbito de la ciberseguridad.
7. Reforzar las relaciones con las Administraciones Públicas y sector públco concernidas en el ámbito de la ciberseguridad.
8. Realizar en apoyo del Comité Especializado de Situación la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis.
9. Contribuir a la organización de la contribución de recursos a la Seguridad Nacional de responsabilidad del Consejo de Seguridad Nacional en el ámbito de la ciberseguridad.
10. Aprobar sus propias normas de régimen interno y de funcionamiento.
11. Todas aquellas otras funciones que le atribuya el ordenamiento jurídico o que le encomiende el Consejo de Seguridad Nacional.

Quinto. Composición:

1. Presidencia: ejercida por el Secretario de Estado Director del Centro Nacional de Inteligencia.
2. Vicepresidencia: ocupada por el Director del Departamento de Seguridad Nacional.
3. Vocales: figuras de apoyo del consejo.
4. Secretaría Técnica y órgano de trabajo permanente del Consejo y otros apoyos a la presidencia: De apoyo al presidente, desempeñada por el Departamento de Seguridad Nacional, el Secretario será designado por el Presidente.

Sexto. Emisión de informes:

1. Los informes únicamente podrán ser emitidos a instancia del Consejo de Seguridad Nacional o a iniciativa del propio Consejo.
2. En todo caso, serán elevados a la consideración y, en su caso, conformidad del Consejo de Seguridad Nacional, a través del Presidente.

Séptimo. Utilización de los mecanismos de enlace y coordinación:

1. El Consejo utilizará los mecanismos de enlace y coordinación establecidos por el Consejo de Seguridad Nacional en el Acuerdo de 20 de enero de 2017.
2. Según lo dispuesto en el apartado quinto del citado Acuerdo del Consejo de Seguridad Nacional de 20 de enero de 2017, los miembros del Consejo velarán por la coherencia y armonización de la información a trasladar en el seno del Consejo.
3. El Dpto. de Seguridad Nacional, según lo establecido (artículo 20.4 de la Ley 36/2015, de 28 de septiembre) mantendrá activados los mecanismos de enlace y coordinación con los organismos del conjunto de las Administraciones Públicas necesarios para que el Sistema de Seguridad Nacional ejerza sus funciones y cumpla con sus objetivos.

Octavo. Grupos de trabajo:

1. El Consejo podrá crear grupos de trabajo para la asistencia técnica en el desempeño de sus funciones, con la composición, objetivos, cometidos y calendario para su realización
2. Los grupos de trabajo responderán ante el Consejo del resultado de sus cometidos y actividades que desarrollen, y serán coordinados por el Departamento de Seguridad Nacional.
3. El régimen de funcionamiento de los grupos de trabajo que se constituyan se determinará en las normas de régimen interno de las que se doten.

Noveno. Reuniones: El Consejo se reunirá presencialmente o a distancia a iniciativa del Presidente, mínimo con carácter bimestral, o cuantas veces lo considere oportunas.

***Ilustración 13**: Acuerdo de regulación del Consejo Nacional de Ciberseguridad 2018*[62]*.*

[62] MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES PÚBLICAS. (23 de enero de 2018). Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. *BOE* nº 20, sección, pág. 8186-90, Gobierno de España. Recuperado de: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-799.pdf

2) Comité Especializado de Ciberseguridad:

El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional y en concreto a su presidente. La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad[63] (Implantación paulatina y organizada hasta alcanzar sus objetivos).

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

3) Comité Especializado de Situación: El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad.

El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno[64] (Implantación paulatina y organizada hasta alcanzar sus objetivos).

I.5.- CAPACIDADES OPERATIVAS EN ESPAÑA EN MATERIA DE CIBERSEGURIDAD

Normalmente los **ciberataques** comparten unas caracterícas comunes, como el bajo coste, el fácil empleo, la efectividad y el bajo riesgo para el atacante. Los agentes que pueden realizar alguna acción en el ciberespacio son variados, yendo desde los propios Estados, hasta los grupos extremistas (ideológicos o políticos), pasando por el crimen organizado o las actuaciones delictivas individuales. De todos modos, por su impacto podría destacarse a las organizaciones delictivas relacionadas con el robo de tarjetas de crédito o certificados digitales, el fraude

[63] CONSEJO DE SEGURIDAD NACIONAL, ESPAÑA. (5 de diciembre de 2013). Ob., cit., p. 44.
[64] Ibídem., p. 45.

telemático, el blanqueo de dinero y el robo de identidades asociado a la inmigración ilegal. Desde el lado del Estado, puede aparecer el espionaje industrial y el *Hawking* político (como por ejemplo los ataques de denegación de servicio entre China y Japón, India y Pakistán o entre árabes e israelíes), o los servicios de inteligencia o unidades cibernéticas de las Fuerzas Armadas, ya que manejan información sensible y pueden especializarse con recursos técnicos para actuar contra otros sistemas de seguridad, sobre todo en tiempo de crisis o conflictos. Comentario aparte merece el ciberterrorismo destacado por el uso de ciberataques con efectos catastróficos y pánico generalizado[65].

Ante esta amenaza y para garantizar el uso seguro de redes y sistemas de comunicación, el Gobierno español promovió unas líneas de acción concretas, dando como resultado el nacimiento de la **Estrategia de Ciberseguridad Nacional**[66], aprobada por el Consejo de Seguridad Nacional el 5 de diciembre de 2013, que responde a la creciente necesidad de preservar la seguridad en el ciberespacio por su enorme repercusión en cuestiones que afectan a la seguridad nacional, a la competitividad de la economía, el progreso y la prosperidad de nuestra sociedad. A continuación veremos algunas de las capacidades operativas indicadas por MOURE[67] y ABAD[68] que han sido emprendidas en este ámbito a nivel ministerial:

I.5.1.- Ministerio de Hacienda y Función Pública

Los ciudadanos empleamos, cada vez más, las tecnologías de la información y comunicación (TIC) como herramienta para realizar nuestras actividades diarias, por lo que se han convertido en un pilar fundamental en nuestro que hacer

[65] CANDAU ROMERO, J. (2011). Estrategias nacionales de ciberseguridad. Ciberterrorismo. Cap. VI. En IEEE, Instituto Español de Estudios Estratégicos, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Cuaderno de seguridad* nº 149 (pp. 259-322). Madrid: Ministerio de Defensa. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[66] CONSEJO DE SEGURIDAD NACIONAL, ESPAÑA. (5 de diciembre de 2013). Ob., cit., pp. 1-55.

[67] MOURE COLÓN, F. (2014). Armonización de las líneas de acción de la estrategia integral de seguridad de la comunidad internacional: aportación española (pp. 391-396). Madrid: Dykinson.

[68] ABAD ARRANZ, M. A. (2016). Capacidades de ciberseguridad en España. En MARTÍN MINGUIJÓN, A. R. y MORÁN MARTÍN, R. (Coords.) Seguridad, Extranjería y otros estudios histórico-jurídicos (pp. 145-154). Madrid: Iustel.

cotidiano.

Las Administraciones Públicas no son ajenas a la innovación tecnológica para la atención al ciudadano y para su propia gestión por lo que el Ministerio de Hacienda y Función Pública (antes Hacienda y Administraciones Públicas) junto con el Ministerio de Energía, Turismo y Agenda Digital (antes Industria, Energía y Turismo) iniciaron en mayo de 2012 un proceso abierto, transparente y colaborativo que culminó, el 15 de febrero de 2013, con la aprobación de la "Agenda Digital para España"[69], como la estrategia del Gobierno para desarrollar la economía y la sociedad digital en nuestro país. Esta estrategia se configura como el paraguas de todas las acciones del Gobierno en materia de Telecomunicaciones y de Sociedad de la Información. Además marca la hoja de ruta en materia de TIC y de Administración Electrónica para el cumplimiento de los objetivos de la Agenda Digital para Europa en 2015 y en 2020.

Los ciberincidentes y sucesos en empresas del sector público son gestionados por CCN-CERT y son de gran valor para ver la evolución de los ciberataques.

"Hallazgos más significativos de 2017 en materia de ciberseguridad:

- Los actores estatales y los criminales profesionales continúan siendo la amenaza más importante, causando el mayor daño.
- Los ciberataques se han utilizado para influir en los procesos democráticos.
- La ciberguerra, los ciberconflictos y la guerra híbrida se hacen cada día más presente en el mundo, siempre apoyado por acciones en el ciberespacio.
- Las vulnerabilidades de *Internet of Things* han propiciado la existencia de ataques disruptivos que justifican la necesidad de mejorar la resiliencia digital.

[69] MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, ESPAÑA. (2017). Agenda Digital para España. Recuperado de: http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx

- Muchas organizaciones dependen de un número limitado de proveedores extranjeros de servicios de infraestructuras digitales, lo que significa que el impacto social de eventuales interrupciones podría ser notable.

- La capacidad de recuperación de las personas y las organizaciones sigue a la zaga de las crecientes amenazas"[70].

I.5.2.- Ministerio de Energía, Turismo y Agenda Digital

La Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, desarrolla el empleo de las tecnologías de la información con el "*Plan Avanza"*[71]. La industria de la ciberseguridad ha experimentado en los últimos años un notable crecimiento derivado del incremento en la cantidad y en la magnitud de los incidentes de ciberseguridad. Esta tendencia se presenta asimismo como una oportunidad para la iniciativa privada de desarrollar una industria capaz de satisfacer la cada vez mayor demanda de soluciones de ciberseguridad. La consolidación de la Estrategia española de Ciberseguridad, que identifica las amenazas, define una organización con una serie de centros de referencia y una coordinación entre las Administraciones, empresas y terceros países. Con estos avances realizados en los años anteriores, hacen previsible el cumplimiento de los objetivos en materia de seguridad planteados por la Agenda Digital para Europa[72].

La **Agenda Digital** se estructura en torno a seis grandes objetivos desarrollados mediante planes específicos. El Plan de Confianza Digital, hace suyo el mandato de la Estrategia Europea de Ciberseguridad y de la Estrategia de Seguridad Nacional para avanzar en los objetivos conjuntos de construir un clima de confianza para contribuir al desarrollo de la economía y la sociedad digital; disponer de un ciberespacio abierto, seguro y protegido; garantizar un uso seguro

[70] CCN-CERT IA-09 (Mayo de 2018). Centro Criptológico Nacional (CCN). Ciberamenazas y tendencias, Pág. 8. Recuperado de: https://lnkd.in/dHJa2uc

[71] CONSEJO DE MINISTROS, ESPAÑA. (16 de julio de 2010). Acuerdo de la Estrategia 2011-2015 del Plan Avanza.

[72] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, ESPAÑA. (22 de junio de 2012) Informe de recomendaciones del Grupo de expertos de Alto Nivel de la Agenda Digital para España. (pp. 51-52). Recuperado de: http://www.minetur.gob.es/telecomunicaciones/es-es/novedades/documents/informe-recomendaciones-ade.pdf

de las redes y los sistemas de información, y responder además a los compromisos internacionales en materia de ciberseguridad. Dicho Plan concreta en su Eje IV el reforzar las capacidades de prevención, detección y respuesta frente a los ciberataques a través del Instituto Nacional de Tecnologías de la Comunicación (INTECO) como un centro de referencia especializado en materia de ciberseguridad.

El **INTECO** fundado en 2006, cambió de denominación en 2014 y pasó a llamarse **INCIBE** (Instituto Nacional de Ciberseguridad de España)[73], sociedad dependiente del Ministerio de Energía, Turismo y Agenda Digital a través de la Secretaría de Estado y para la Sociedad de la Información y Agenda Digital (SESIAD). El INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional y es una referencia para desarrollar la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas.

En el seno del INCIBE opera el centro de respuesta a incidentes de ciberseguridad ("C*omputer Emergency Response Team*" CERT) de Seguridad e Industria (CERTSI)[74], que por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015 es el CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes de ciberseguridad. El CERTSI ofrece capacidad tecnológica y de coordinación, de forma continuada 24 horas al día, 7 días a la semana, en tres ámbitos diferenciados: Ciudadanos y empresas; Instituciones afiliadas a la RedIRIS; y Operadores estratégicos y de infraestructuras críticas. En este centro tiene especial relevancia la participación de agentes de la Oficina de Coordinación Cibernética (OCC) del Ministerio del Interior, que permiten trasladar de forma ágil los casos constitutivos de delito

[73] Desde el 28 de octubre de 2014, el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) pasa a llamarse Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE), según el acuerdo adoptado en Junta General del 27 de octubre de 2014. Con dicho cambio de denominación e imagen, INCIBE proyecta una identidad acorde con su orientación estratégica y posicionamiento como centro nacional de referencia en ciberseguridad. Recuperado de: https://www.incibe.es/que-es-incibe

[74] El CERTSI se constituyó en el año 2012 a través de un Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado. Recuperado de: https://www.certsi.es/

telemático a las unidades técnicas de las FCSE.

I.5.3.- Ministerio de la Presidencia

El **Centro Nacional de Inteligencia (CNI)** adscrito al Ministerio de la Presidencia[75], es un organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión, incluidas las ciberamenazas. Cuenta con la Oficina Nacional de Seguridad, (ONS)[76] y el Centro Criptológico Nacional (CCN)[77]. Dentro del CCN se encuentran integrados los CERT, que trabajan en la seguridad de los sistemas y en evitar o minimizar los ataques que se produzcan contra éstos. El CCN-CERT se creó en 2006 y es competente de la gestión de ciberincidentes que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para España y a cualquier sistema clasificado, para contribuir a la mejora de la ciberseguridad, siendo el centro de alerta y respuesta nacional para responder a los ciberataques y afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes o centros de operaciones de ciberseguridad existentes[78].

I.5.4.- Ministerio de Defensa

El Ministerio de Defensa dispone de una política de seguridad con responsabilidades sobre sistemas que manejan información clasificada. Estas

[75] Según su nuevo estatus regulador, Real Decreto 240/2013, de 5 de abril, por el que se aprueba el estatuto del personal del Centro Nacional de Inteligencia. *Boletín Oficial del Estado BOE* nº 89, de 13 de abril de 2013, pp. 27605-27666.

[76] Creado en 1983, como órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relacionados con la protección de la Información Clasificada.

[77] MINISTERIO DE DEFENSA, ESPAÑA. (19 de marzo de 2004). Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. para preservar la seguridad de los sistemas de las tecnologías de la información de la Administración. *Boletín Oficial del Estado (BOE)* nº 68, pp. 12203-12204. Recuperado de: https://www.boe.es/boe/dias/2013/04/13/pdfs/BOE-A-2013-3907.pdf

[78] Funciones que quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

responsabilidades están distribuidas entre la Dirección General de Infraestructuras, el Estado Mayor de la Defensa (EMAD) y los Cuarteles Generales de los tres Ejércitos. El Jefe del EMAD (JEMAD), ejerce la dirección, planificación y coordinación de la capacidad de ciberdefensa para los sistemas de comunicaciones e información de las Fuerzas Armadas y la ejecución de la respuesta y explotación, y tiene bajo su dirección el Mando Conjunto de Ciberdefensa (MCCD). También encuadrado en la Subdirección General de Tecnologías de la Información y Comunicaciones trabaja el Centro de Operaciones de Seguridad de la Información del Ministerio de Defensa (COSDEF)[79]. En enero de 2011 el JEMAD elaboró el documento "Visión de la Ciberdefensa Militar"[80], en el cual se incluye al Ciberespacio como uno de los dominios de enfrentamiento, siendo los otros tierra, mar, aire y espacio exterior. Posteriormente, en julio de 2011, el JEMAD aprueba el "Concepto de la Ciberdefensa Militar" (CDM) en el que se establecen los principios, objetivos y retos de la Ciberdefensa en el ámbito militar, define la terminología, realiza una valoración de la capacidad, y ordena la elaboración de un Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar[81].

El Mando Conjunto de Ciberdefensa surge con el cometido, entre otros, de: garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios; obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad; ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional[82].

[79] Vid. *Boletín Oficial del Ministerio de Defensa (BOD)* nº 251, de 28 de diciembre de 2011 (pp. 33507-33510). Instrucción 96/2011 del Secretario de Estado de Defensa por la que se crea el COSDEF.

[80] ZEA PASQUÍN, F.(marzo de 2013) Ciberdefensa Militar. *Revista Española de Ciberdefensa.* Núm 293. pp. 48-40. Recuperado de: http://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-293-ciberdefensa.pdf

[81] Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar de 12 julio 2012. Vid. PRIETO OSÉS, R & OTROS. (abril de 2013). *Guerra cibernética: Aspectos organizativos*. XXXIII curso de Defensa Nacional. CESEDEN. Madrid.

[82] El MCCD se creó el 19 de febrero de 2013, por Orden Ministerial 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Recuperado de: http://www.emad.mde.es/CIBERDEFENSA/

I.5.5.- Ministerio del Interior

Al Ministerio del Interior le corresponde, entre otras, la preparación y ejecución de la política del Gobierno en relación con la administración general de la seguridad ciudadana y la promoción de las condiciones para el ejercicio de los derechos fundamentales, especialmente en relación con la libertad y seguridad personal, en los términos establecidos en la CE y en las leyes que los desarrollen, por lo que tiene asignadas competencias de gran importancia para el aseguramiento de una adecuada ciberseguridad en España, especialmente en materia de sistemas de información y comunicaciones.

Para desarrollar estas competencias el Ministerio del Interior cuenta con una estructura coordinada por la Secretaría de Estado de Seguridad y la Subsecretaria del Ministerio del Interior. Esta estructura fue modificada en julio de 2017 para dar respuesta a la situación actual[83]. Lo que se busca con estas medidas es actuar con mayor eficacia e innovación como elemento fundamental de fortalecimiento de la seguridad, ya que han aparecido y seguirán apareciendo modalidades delictivas basadas en las tecnologías y la era de la información (Internet y análogos).

El Ministerio del Interior da prioridad siempre a la seguridad de las personas y busca mejorar notablemente los resultados de la lucha contra la criminalidad basándose en los medios, preparación y coordinación dando como resultado la efectividad en las actuaciones. El ministro lo denominó: “Políticas de Seguridad para las Personas”, dentro del plan de Política de Seguridad Nacional para el siglo XXI. Un conjunto de iniciativas dirigidas a hacer frente a las amenazas que se ciernen sobre la pacífica convivencia con el fin de garantizar a los españoles la libertad y la seguridad por igual grado y de esta forma con una estructura actualizada y con la innovación como elemento crucial, incrementarán sus éxitos ante los nuevos retos en materia de seguridad[84].

[83] MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA, ESPAÑA. (29 de julio de 2017). Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. *Boletín Oficial del Estado (BOE) nº. 180, pp. 70439-70468.* Recuperado de: https://www.boe.es/boe/dias/2017/07/29/pdfs/BOE-A-2017-9013.pdf

[84] MINISTERIO DEL INTERIOR, ESPAÑA. (28 de julio de 2017). El Ministerio del Interior modifica la estructura de la Policía Nacional y de la Guardia Civil para afrontar con mayor eficacia los nuevos retos de seguridad. Nota de prensa. Recuperado de: http://www.interior.gob.es/prensa/noticias/-

La reforma que recoge el Real Decreto 770/2017, introduce cambios tanto en la estructura como en la organización de las Direcciones Generales de la Guardia Civil y la Policía Nacional, para afrontar la amenaza del terrorismo yihadista y el escenario de la globalización de la delincuencia. La delincuencia ha evolucionado hacia entornos digitales que obligan a realizar ajustes para garantizar que también frente a los nuevos delitos electrónicos se puede ofrecer al conjunto de los españoles mayores garantías de seguridad. Además, en las últimas fechas España, al igual que otros países, ha sido objeto de graves ciberataques y las delincuencias común y organizada han incrementado sus actuaciones en el ciberespacio[85].

Este escenario ha llevado a que en la Guardia Civil se cree un nuevo "Mando de Información, Investigación y Ciberdelincuencia" junto con los tradicionales "Mando de Operaciones Territoriales", "Mando de Personal y Formación" y "Mando de Apoyo e Innovación". También la Policía Nacional diversifica su estructura en Jefatura Central de Seguridad Ciudadana y Coordinación; Jefatura Central de Información, Investigación y Ciberdelincuencia; Jefatura Central de Recursos Humanos y Formación, y Jefatura Central de Logística e Innovación.

A continuación vemos los instrumentos más relevantes relacionados con la ciberseguridad:

- **Centro Nacional para la protección de las Infraestructuras y Ciberseguridad** (CNPIC). Es el órgano que se encarga de impulsar, coordinar y supervisar las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con las infraestructuras críticas. Esta Secretaría y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información suscribió un acuerdo en el que, entre otros aspectos, se sentaban las bases para la colaboración del CNPIC con el Instituto Nacional de Ciberseguridad

/asset_publisher/GHU8Ap6ztgsg/content/id/7578978

[85] PERIÓDICO DIGITAL, LA INFORMACIÓN. (12 de mayo de 2017) España ha resuelto más de 50.000 ciberataques en lo que va de año, 247 críticos. Recuperado de https://www.lainformacion.com/espana/Espana-resuelto-ciberataques-operadores-estrategicos_0_1025597841.html

(INCIBE) en materia de respuesta a incidentes para las tecnologías de la información de las infraestructuras críticas ubicadas en España, convirtiendo al INCIBE en una herramienta de apoyo al CNPIC en la gestión de incidentes de ciberseguridad. Ambas entidades pusieron en marcha un Equipo de Respuesta a Incidentes de Seguridadespecializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica. De este modo, este Equipo de Respuesta se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional. En caso de que una Infraestructura Crítica sufra un problema de seguridad cibernético, el operador responsable de la misma podrá beneficiarse de los servicios del equipo de respuesta, informando de la incidencia a través del Punto de Contacto Único habilitado para esta finalidad. Además el CNPIC colabora con el Centro Criptológico Nacional (CCN) y presenta una serie de guías de interés para la seguridad de los sistemas de control industrial, también conocidas como "SCADA"[86].

- **Grupo de Delitos Telemáticos de la Guardia Civil** (GDT). Este Grupo depende de la Unidad Central Operativa de la Guardia Civil (UCO), su origen se remonta a 1996, para atender a las denuncias de los entonces llamados delitos informáticos. Posteriormente con la socialización de Internet y el crecimiento de los hechos delictivos se amplió su abanico de competencias de investigación, en todo el territorio nacional, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. También en cada una de las provincias de España se encuentran desplegados los Equipos de Investigación Tecnológica (EDITE)[87]. A su vez, la UCO depende de la Jefatura de Policía Judicial del nuevo Mando de Información, Investigación y Ciberdelincuencia.

[86] CNPIC. (2017). Centro Nacional para la Protección de las Infraestructuras y Ciberseguridad. Recuperado de: http://www.cnpic.es/Ciberseguridad/index.html

[87] GRUPO DE DELITOS TELEMÁTICOS DE LA GUARDIA CIVIL. (2017). GDT. Recuperado de: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

- **Brigada de Investigación Tecnológica de la Policía Nacional** (BIT). Está encuadrada en la Unidad de Investigación Tecnológica y le corresponde, en su zona de actuación, la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones[88]. Depende de la Comisaría General de la Policía Judicial y a su vez de la Jefatura Central de Información, Investigación y Ciberdelincuencia.

- **Grupo de Ciberterrorismo (GCT) y Unidad de Ciberseguridad (UCS) de la Guardia Civil**. Tanto la Guardia Civil como la Policía Nacional disponen de unidades especializadas dentro de sus respectivos Servicios de Información que completan las capacidades del Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado (CITCO) en materia de ciberterrorismo de la Secretaría de Estado de Seguridad.

La respuesta ante la amenaza del uso de Internet y de las TIC por parte de organizaciones terroristas, se convirtió desde el año 2000 en una de las prioridades de la Jefatura de Información de la Guardia Civil materializándose en la formación del primer embrión del Grupo de Ciberterrorismo en noviembre de 2002 que se conformó como tal en 2007, incorporándose en el nuevo Grupo otras unidades de claro perfil tecnológico como son los Grupos Técnico Informativo, de Interceptación de Telecomunicaciones y de Informática Forense aumentando sus capacidades de respuesta de la Guardia Civil. Paralelamente, en diciembre de 2012, se constituyó la Unidad de Ciberseguridad integrada por un equipo humano de alta cualificación y dotado de novedosos sistemas tecnológicos y herramientas informáticas[89].

[88] BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA POLICÍA NACIONAL. (2017). BIT. Recuperado de: https://www.policia.es/org_central/judicial/udef/bit_alertas.html

[89] ORTIGOSA, A. y HERNÁNDEZ GARCÍA, L. F. (2016). Las nuevas amenazas cibernéticas del S.XXI Ciberterrorismo: Nueva forma de subversión y desestabilización. En *Cuadernos de la Guardia Civil. 75 Aniversario. Servicio de Información* (pp. 104-122). Madrid: Centro Universitario de la Guardia Civil. Recuperado de http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/documents/18266_19488.pdf

- **Oficina de Coordinación Cibernética** (OCC). Es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC[90]. La OCC realiza la coordinación técnica entre el CERTSI y los órganos subordinados de la Secretaría de Estado de Seguridad (CITCO, Guardia Civil, Policía Nacional, Protección Civil y Emergencias). Después de los atentados de París (7 de enero de 2015) la OCC activó un dispositivo extraordinario de ciberseguridad.

I.5.6.- Otros agentes Estatales

- Grupos de trabajo de los proyectos *Rescata, Seguridad y Confianza, usabilidad del DNIe* (Ministerio de Economía, industria y Competitividad).
- Agencia Española de Protección de Datos (Ministerio de Justicia).
- Federación Española de Municipios y Provincias.
- Centro de Operaciones de Seguridad de la Junta de Castilla y León
- Centro de Seguridad TIC de la Comunitat Valenciana "CSIRT-CV".
- Centro de Seguridad de la Información de la Generalitat de Catalunya "CESICAT".
- Centro de respuesta a incidentes de ciberseguridad "AndalucíaCERT"
- Servicio de Alerta Temprana de otras Comunidades Autonómicas y Ayuntamientos.

I.5.7.- Cooperación de organismos con responsabilidad en ciberseguridad

La Estrategia de Ciberseguridad Nacional de 2013, fija en su Línea de Acción 1, la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CCN-CERT, el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Los CERT de las

[90] La Oficina de Coordinación Cibernética fue creada mediante Instrucción del Secretario de Estado de Seguridad 15/2014 de 19 de noviembre.

Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto.

En la parte dedicada a la ciberdefensa específicamente, España participa activamente en el Centro de Excelencia de Ciberdefensa Cooperativa ("*Cooperative Cyber Defence Centre of Excellence*", CCD COE) que la OTAN ha establecido en Tallín, Estonia, tras la firma del MoU del 14 de mayo de 2008. El CCD COE es una organización multinacional que proporciona I+D y servicios de formación a la OTAN, entre otras cosas. Está abierto a la participación de todos los miembros de la OTAN y además puede firmar acuerdos con organizaciones ajenas a la OTAN, como universidades, empresas, etc. Centrará su trabajo en las siguientes áreas fundamentales de la Ciberdefensa:

- Desarrollo de doctrinas y conceptos.
- Formación y concienciación.
- Investigación y desarrollo.
- Análisis y lecciones aprendidas.
- Consulta.

En el marco de la UE, el Centro Europeo de Cibercrimen (EC3), dependiente de Europol, se ocupa de los delitos relacionados con el ciberterrorismo, desde enero de 2013, centrándose principalmente en los delitos de fraude económico, los relacionados con ataques informáticos a empresas o infraestructuras críticas y explotación sexual infantil, así como a la recogida de información de inteligencia, de una gran variedad de fuentes tanto públicas como privadas a fin de alimentar una base de datos policiales, que permita facilitar información a los países miembros[91].

El pasado 23 de Mayo del 2018 se ha firmado un convenio de colaboracion entre las cuatro principales organizaciones europeas de ciberseguridad, el Mou principalmente intentara aprovechar las sinergias de las organizaciones en

[91] EUROPOL. (2013). European Cybercrime Centre (EC3). Recuperado de: https://www.europol.europa.eu/ec3

ciberseguridad y ciberdefensa basandose en la buena relación y confianza entre estas, se intentara garantizar el mejor uso posible de los recursos y asi desarrollar un doble valor del apoyo que estas proporcionan a organizaciones y estados miembros. La cooperacion se centra principalmente en cinco areas: intercambio de información, educacion y entrenamiento, ejercicios ciberneticos, cooperación técnica y asuntos estátegicos y administrativos.

"The European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) today signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations". [92]

I.6.- ACTUALIDAD DEL CIBERCRIMEN Y TERRORISMO EN ESPAÑA

I.6.1.- Evolución del Cibercrimen en España

El crecimiento del cibercrimen en España lo podríamos denominar como "bestial", somos el noveno país de Europa en el ranking de ciberdelitos. Hemos pasado de de 35.000 delitos registrados en el año 2011 a 66.584 en el año 2016 y esto sigue, los expertos no le ven freno. El propio director de Europol, ROB WAINWRIGHT comenta que ésta es una amenaza real, constante y creciente, siendo la piedra angular de este crimen la difusión del malware.

La falibilidad de estos preceptos da sentido a las técnicas de *CounterCraft: "Nuestro objetivo es pensar como los críminales y ponerles trampas que nos permiten extraer sus datos",* explica BARROSO*. "¿Quiénes son? ¿Cómo han entrado? ¿Con qué herramienta? ¿Qué pretenden?"*

Para responder a estas preguntas, la startup crea realidades paralelas:

[92] ENISA (23 mayo de 2018), Four EU cybersecurity organisations enhance cooperation. Recuperado de: https://www.enisa.europa.eu/news/enisa-news/four-eu-cybersecurity-organisations-enhance-cooperation

introducen archivos con información falsa, crean personas ficticias dentro de la empresa, cuyos ordenadores son vulnerables... *"Es como esas fotos de tanques hinchables de la Segunda Guerra Mundial. Pero nosotros simulamos personas, máquinas, servicios o páginas web"*[93].

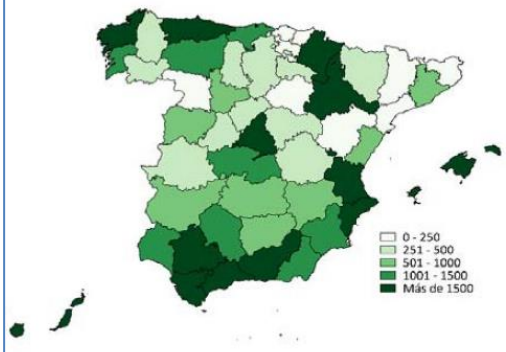
Vamos a mostrar ahora unas ilustraciones extraídas del Informe de Cibercriminalidad realizado por el Ministerio del Interior Español en 2016, de la Fundación ESYS (ilustraciones 14 a 30).

Hechos conocidos:	66.586	
Esclarecimiento:	20.453	**30,7%**
Detenciones/invest:	4.802	
CCAA	Hechos	
ANDALUCÍA	13.052	
MADRID (COMUNIDAD DE)	10.564	
COMUNITAT VALENCIANA	9.043	
CASTILLA Y LEON	4.682	
GALICIA	4.561	
EXTRANJERA	4.381	
CASTILLA - LA MANCHA	3.184	
CANARIAS	2.934	
BALEARS (ILLES)	2.892	
ARAGÓN	2.066	
NAVARRA (COMUNIDAD FORAL DE)	1.911	
ASTURIAS (PRINCIPADO DE)	1.714	
MURCIA (REGION DE)	1.445	
EXTREMADURA	1.327	
CANTABRIA	1.307	
CATALUÑA	772	
PAÍS VASCO	289	
RIOJA (LA)	254	
CIUDAD AUTÓNOMA DE CEUTA	139	
CIUDAD AUTÓNOMA DE MELILLA	69	

***Ilustración 14**: Hechos denunciados de cibercriminalidad*[94].

[93] HIDALGO PÉREZ, M. (19 de diciembre de 2017). Ob., cit.

[94] GABINETE DE COORDINACIÓN DE ESTUDIOS. (2016). Secretaria de Estado. Ministerio del Interior, Madrid.



Provincias más afectadas:	Hechos
Madrid	10.564
Valencia/València	4.933
Extranjero	4.381
Alicante/Alacant	3.240
Sevilla	2.939
Balears (Illes)	2.892
Coruña (A)	2.373
Málaga	2.105
Palmas (Las)	1.952
Cádiz	1.939
Navarra	1.911
Asturias	1.714
Zaragoza	1.608
Granada	1.564
Pontevedra	1.459
Murcia	1.445
Toledo	1.355
Córdoba	1.335
Cantabria	1.307
Almería	1.249

***Ilustración 15**: Provincias más afectadas*[95].

VICTIMIZACIONES	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.233	3.307	4.540
AMENAZAS Y COACCIONES	6.757	5.291	12.048
CONTRA EL HONOR	691	934	1.625
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	22	10	32
DELITOS SEXUALES	325	569	894
FALSIFICACIÓN INFORMÁTICA	876	909	1.785
FRAUDE INFORMÁTICO	19.056	13.515	32.571
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	623	328	951
Total VICTIMIZACIONES	**29.583**	**24.863**	**54.446**

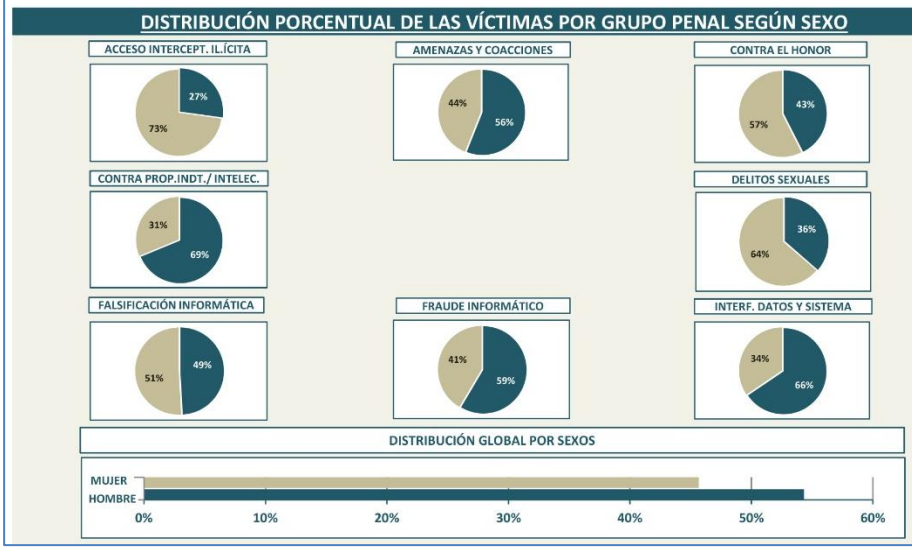
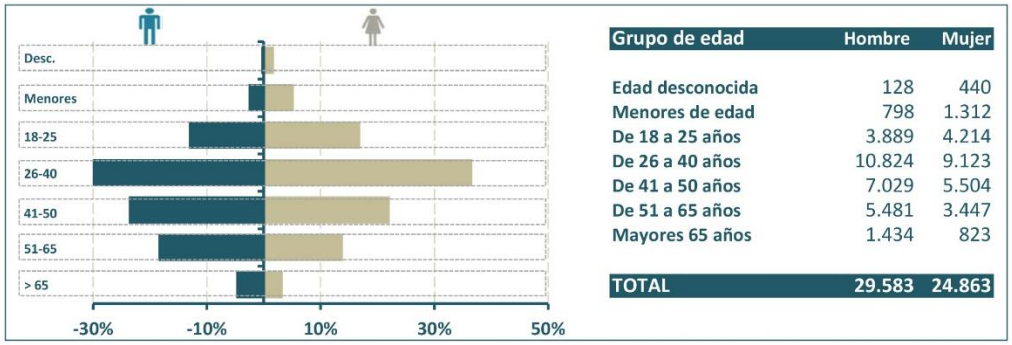


***Ilustración 16**: Datos estadísticos de cibercriminalidad: Victimización registrada según grupo penal y sexo*[96].

[95] Ibídem.
[96] Ibídem., p. 35.



Grupo de edad	Hombre	Mujer
Edad desconocida	128	440
Menores de edad	798	1.312
De 18 a 25 años	3.889	4.214
De 26 a 40 años	10.824	9.123
De 41 a 50 años	7.029	5.504
De 51 a 65 años	5.481	3.447
Mayores 65 años	1.434	823
TOTAL	29.583	24.863

Ilustración 17: *Datos estadísticos de cibercriminalidad: Victimización según grupo edad y sexo*[97]*.*

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	9.922	6.560	16.482
ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES D	8.411	6.471	14.882
AMENAZAS	5.621	4.562	10.183
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	718	2.726	3.444
COACCIONES	1.135	727	1.862
USURPACIÓN DE ESTADO CIVIL	876	909	1.785
INJURIAS	497	821	1.318
ESTAFA BANCARIA	723	484	1.207
ACCESO ILEGAL INFORMÁTICO	514	581	1.095
RESTO	1.166	1.022	2.188
Total VICTIMIZACIONES CIBERCRIMINALIDAD	29.583	24.863	54.446

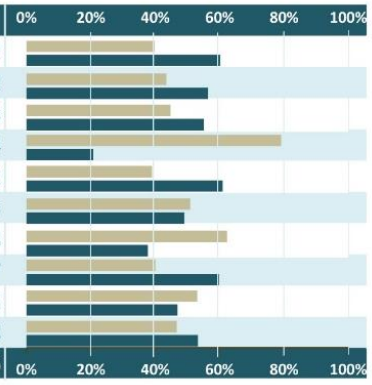


Ilustración 18*: Datos estadísticos de cibercriminalidad: Victimizaciones por título penal y sexo*[98]*.*

[97] Ibídem., p. 35.
[98] Ibídem., p. 36.

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	49.124	90,2%
2.- EXTRANJEROS	5.322	9,8%
2.1.- UNIÓN EUROPEA	1.978	3,6%
Rumanía	614	1,1%
Italia	267	0,5%
Reino Unido	201	0,4%
Alemania	157	0,3%
Francia	152	0,3%
Resto	587	1,1%
2.2.- AMÉRICA	1.230	2,3%
Colombia	207	0,4%
Ecuador	155	0,3%
Brasil	127	0,2%
Resto	741	1,4%
2.3.- ÁFRICA	596	1,1%
Marruecos	391	0,7%
Senegal	46	0,1%
Resto	159	0,3%
2.4.- ÁSIA	226	0,4%
China	81	0,1%
Paquistán	42	0,1%
Resto	103	0,2%
2.5.- RESTO PAÍSES	1.292	2,4%
Ucrania	82	0,2%
Rusia	77	0,1%
Otros	1.133	2,1%
TOTAL	54.446	100%

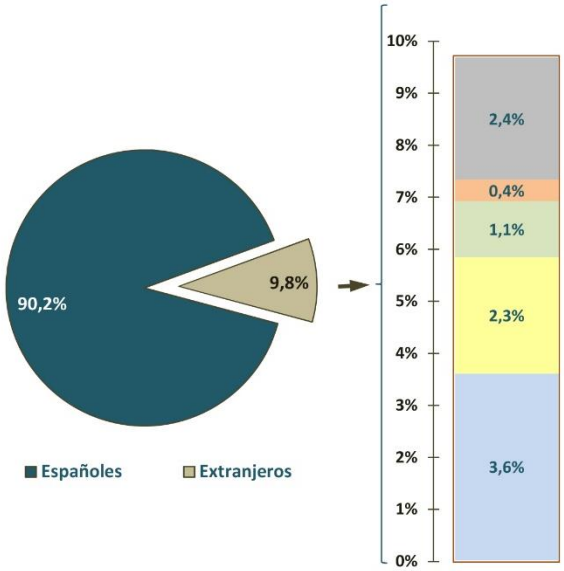


***Ilustración 19**: Datos estadísticos de cibercriminalidad: Nacionalidad de la víctima*[99].

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	1.242	421	1.663
AMENAZAS	730	209	939
PORNOGRAFÍA DE MENORES	377	14	391
USURPACIÓN DE ESTADO CIVIL	179	125	304
ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQ	157	78	235
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	169	63	232
ESTAFA BANCARIA	144	60	204
COACCIONES	151	29	180
CORRUPCIÓN DE MENORES/INCAPACITADOS	114	6	120
RESTO	444	87	531
Total VICTIMIZACIONES CIBERCRIMINALIDAD	3.707	1.092	4.799

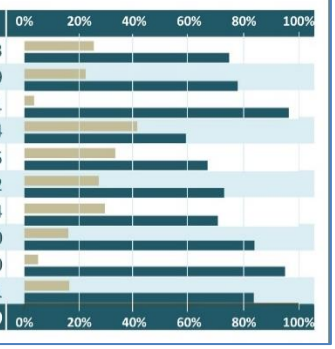
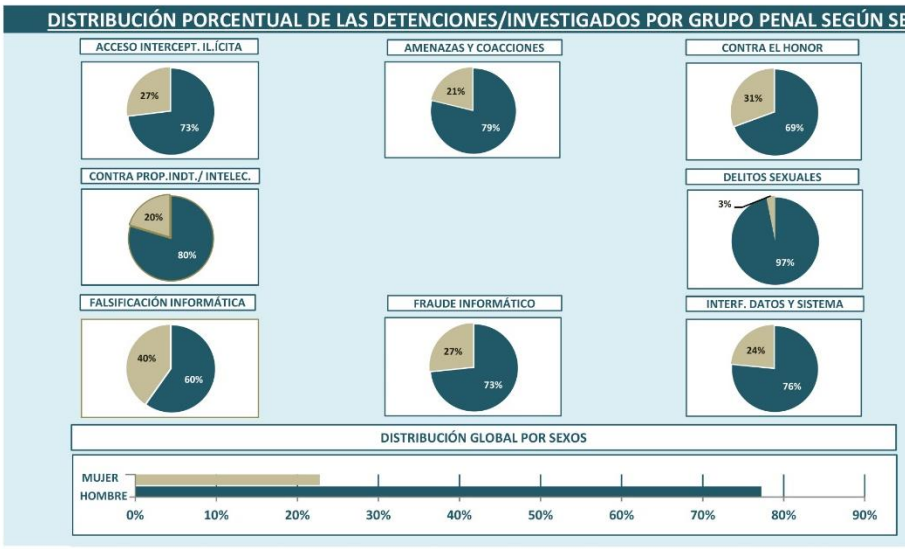


***Ilustración 20**: Datos estadísticos de cibercriminalidad: Detenciones/Investigados por tipología penal y sexo*[100].

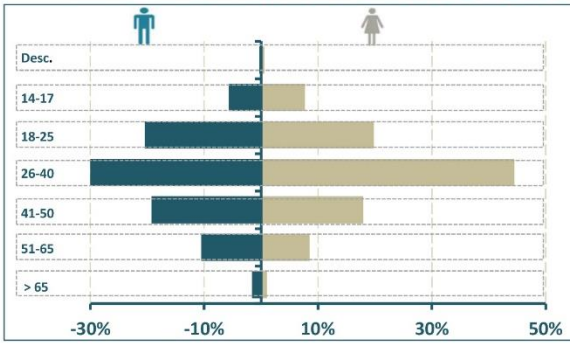
[99] Ibídem., p. 36.
[100] Ibídem., p. 41.

>> 4.10. Detenciones/investigados registrados según grupo penal y sexo. Año 2016

DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	228	84	312
AMENAZAS Y COACCIONES	884	238	1.122
CONTRA EL HONOR	66	29	95
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	98	25	123
DELITOS SEXUALES	673	22	695
FALSIFICACIÓN INFORMÁTICA	189	127	316
FRAUDE INFORMÁTICO	1.543	559	2.102
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	26	8	34
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**3.707**	**1.092**	**4.799**



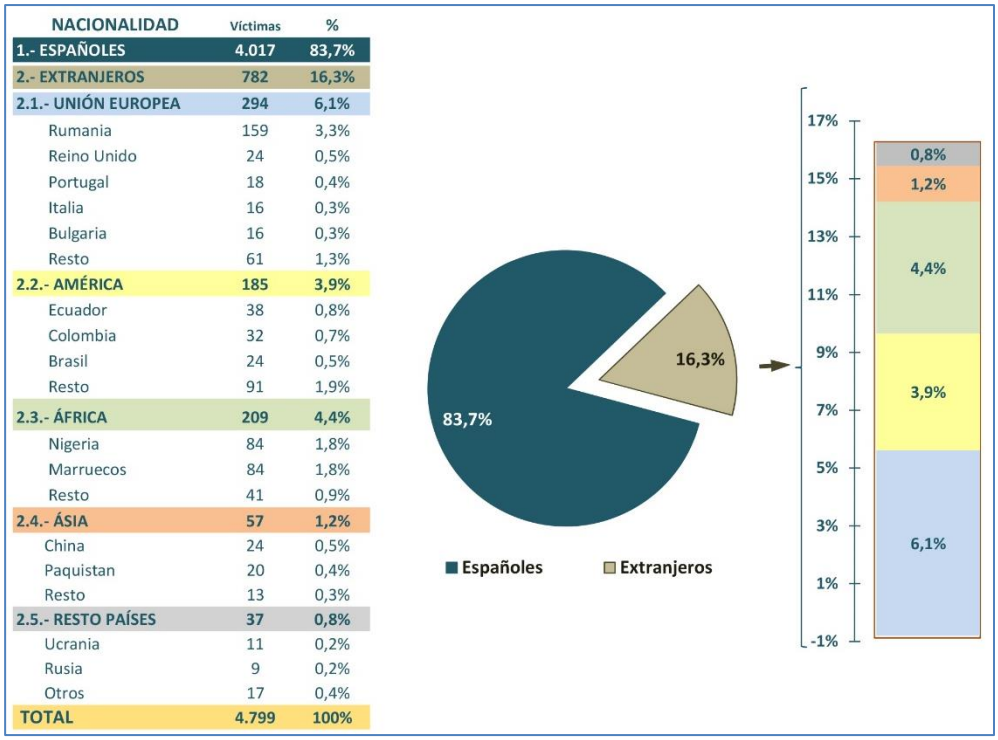
>> 4.11. DETENCIONES/INVESTIGADOS según grupo de edad y sexo. Año 2016



Grupo de edad	Hombre	Mujer
Edad desconocida	12	6
De 14 a 17 años	211	84
De 18 a 25 años	758	216
De 26 a 40 años	1.561	486
De 41 a 50 años	714	196
De 51 a 65 años	391	93
Mayores 65 años	60	11
TOTAL	**3.707**	**1.092**

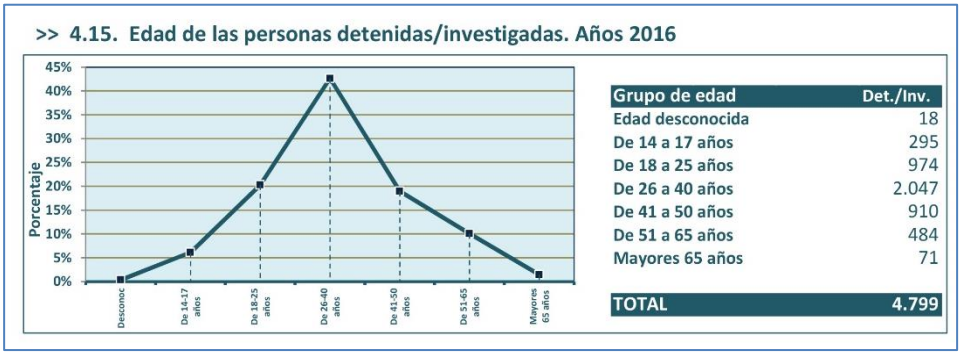
***Ilustración 21**: Datos estadísticos de cibercriminalidad: perfil del responsable*[101].

[101] Ibídem., p. 40.



NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	4.017	83,7%
2.- EXTRANJEROS	782	16,3%
2.1.- UNIÓN EUROPEA	294	6,1%
Rumania	159	3,3%
Reino Unido	24	0,5%
Portugal	18	0,4%
Italia	16	0,3%
Bulgaria	16	0,3%
Resto	61	1,3%
2.2.- AMÉRICA	185	3,9%
Ecuador	38	0,8%
Colombia	32	0,7%
Brasil	24	0,5%
Resto	91	1,9%
2.3.- ÁFRICA	209	4,4%
Nigeria	84	1,8%
Marruecos	84	1,8%
Resto	41	0,9%
2.4.- ÁSIA	57	1,2%
China	24	0,5%
Paquistan	20	0,4%
Resto	13	0,3%
2.5.- RESTO PAÍSES	37	0,8%
Ucrania	11	0,2%
Rusia	9	0,2%
Otros	17	0,4%
TOTAL	4.799	100%

***Ilustración 22**: Datos estadísticos de cibercriminalidad: Nacionalidad de los detenidos/Investigados[102].*

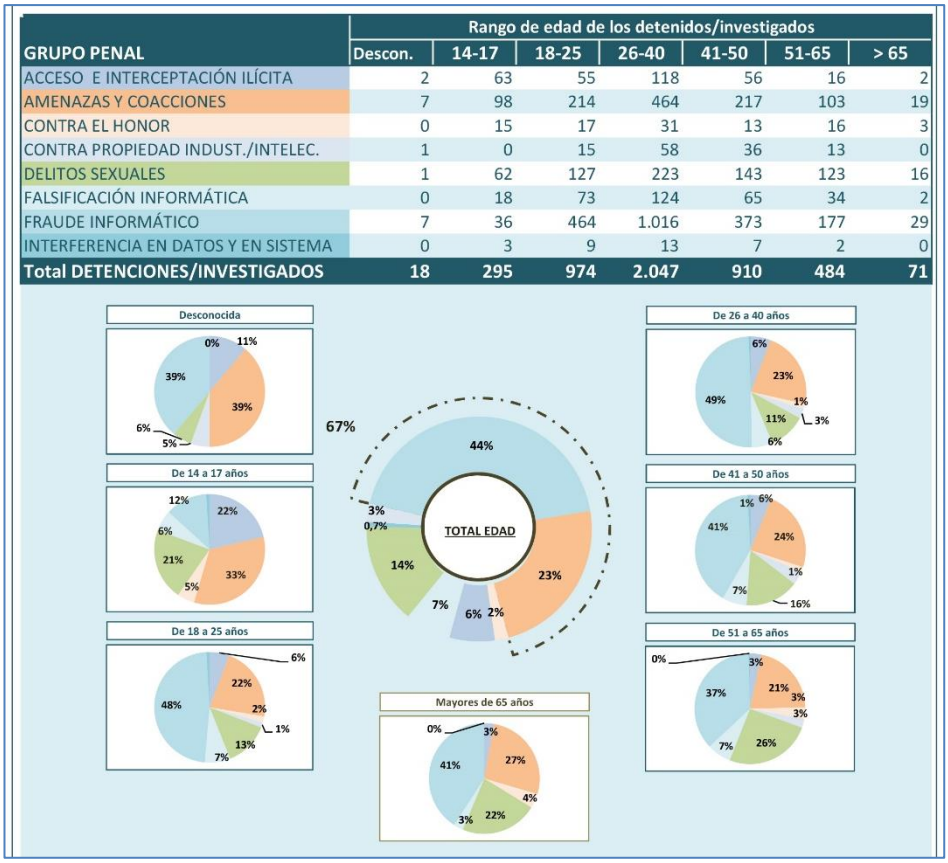


>> 4.15. Edad de las personas detenidas/investigadas. Años 2016

Grupo de edad	Det./Inv.
Edad desconocida	18
De 14 a 17 años	295
De 18 a 25 años	974
De 26 a 40 años	2.047
De 41 a 50 años	910
De 51 a 65 años	484
Mayores 65 años	71
TOTAL	4.799

***Ilustración 23**: Datos estadísticos de cibercriminalidad: Edad de las personas detenidas/investigadas[103].*

[102] Ibídem., p. 41.
[103] Ibídem., p. 42.



GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	2	63	55	118	56	16	2
AMENAZAS Y COACCIONES	7	98	214	464	217	103	19
CONTRA EL HONOR	0	15	17	31	13	16	3
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	15	58	36	13	0
DELITOS SEXUALES	1	62	127	223	143	123	16
FALSIFICACIÓN INFORMÁTICA	0	18	73	124	65	34	2
FRAUDE INFORMÁTICO	7	36	464	1.016	373	177	29
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	9	13	7	2	0
Total DETENCIONES/INVESTIGADOS	**18**	**295**	**974**	**2.047**	**910**	**484**	**71**

***Ilustración 24**: Datos estadísticos de cibercriminalidad: Detenciones/investigados según grupo penal y edad*[104].

La mayoría de los delitos esclarecidos (4.799) son realizados por españoles un 87% aproximadamente, seguidos de los ciudadanos rumanos (294) y Reino Unido (24). En definitiva las fuerzas de seguridad necesitan contar con las mejores herramientas y una legislación más ágil, ya que los delincuentes se saltan las barreras que los agentes deben de respetar.

[104] Ibídem., p. 42.

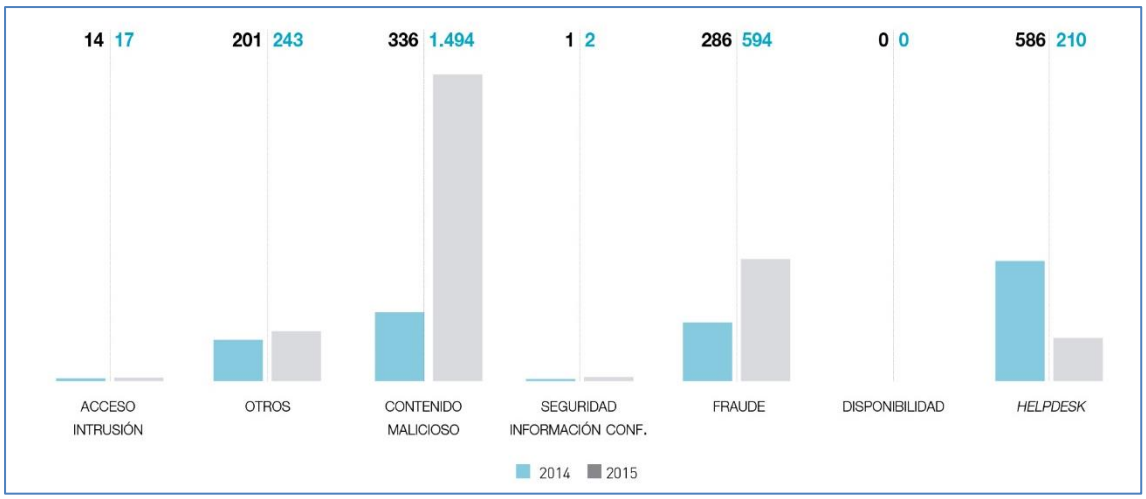


Ilustración 25: *Evolución de la tipología de los incidentes de ciberseguridad para los ciudadanos 2014-15*[105]*.*

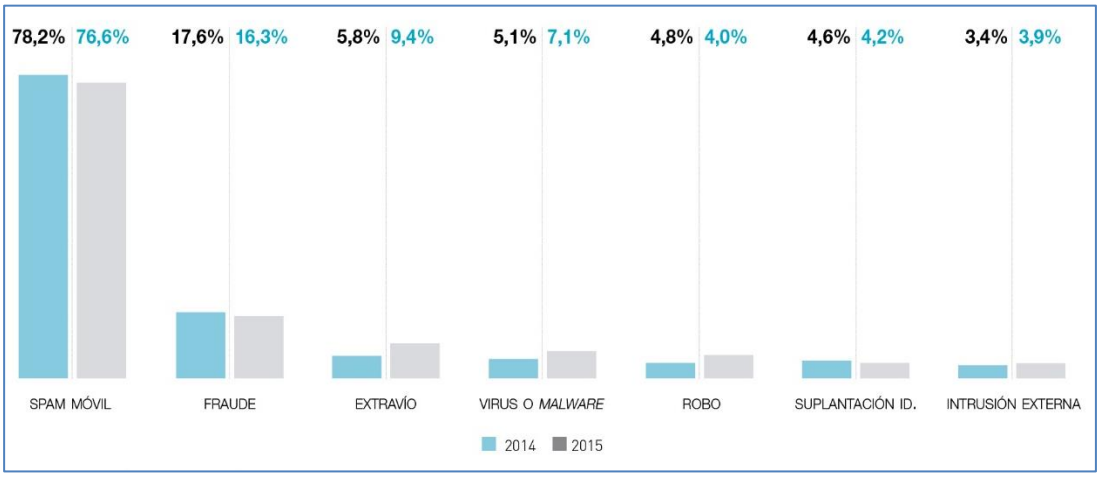


Ilustración 26: *Evolución de la tipología de los incidentes de ciberseguridad para los Smartphone 2014-15*[106]*.*

nº de incidentes	2014	2015	VARIACIÓN 2015/2014
Infraestructuras Críticas	65	111	70,77%
Resto de Empresas	13.236	39.874	201,25%
Total	**13.301**	**39.985**	**200,62%**

Ilustración 27: *Informe anual de la seguridad en España: Evolución de los incidentes registrados por el CERT de seguridad e industria de INCIBE por tipo de empresa 2014-15*[107]*.*

[105] ESYS. (2016). Fundación ESYS. Informe anual de la seguridad, p. 98. Madrid. Recuperado de:http://www.fundacionesys.com/es/system/files/INFORME%20ANUAL%20SEGURIDAD%20ESYS%202016_1.pdf

[106] Ibídem., p. 99.

[107] Ibídem., p. 101.

TIPO DE EMPRESA	CRITICIDAD	2014	2015	VAR. 2015/2014
Infraestructuras Críticas	Alta	57	92	61,40%
	Media	3	7	133,33%
	Baja	5	12	140,00%
Resto de Empresas	Alta	11.365	37.380	228,90%
	Media	23	253	1.000,00%
	Baja	1.848	2.241	21,27%

Ilustración 28: *Informe anual de la seguridad en España: Evolución de los incidentes registrados por el CERT de seguridad e industria de INCIBE por criticidad 2014-15*[108]*.*

Los expertos y muchos entendidos abogan por una posible colaboración entre las fuerzas de seguridad y los fabricantes de tecnología como una posible solución a disminuir los ciberdelitos.

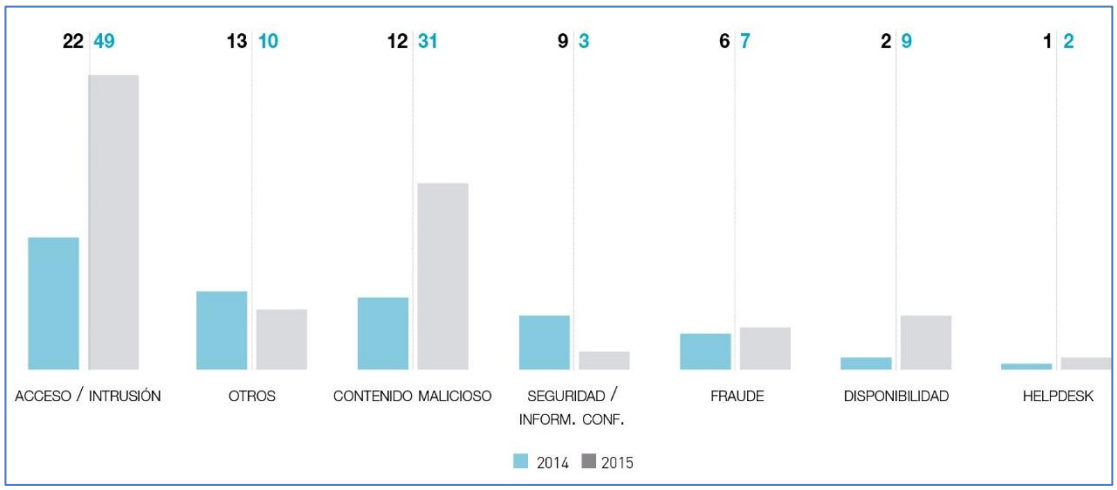


Ilustración 29*: Informe anual de la seguridad en España: Evolución de los incidentes registrados por el CERT de seguridad e industria de INCIBE para las infraestructuras críticas por tipología 2014-15*[109]*.*

[108] Ibídem., p. 102.
[109] Ibídem., p. 103.

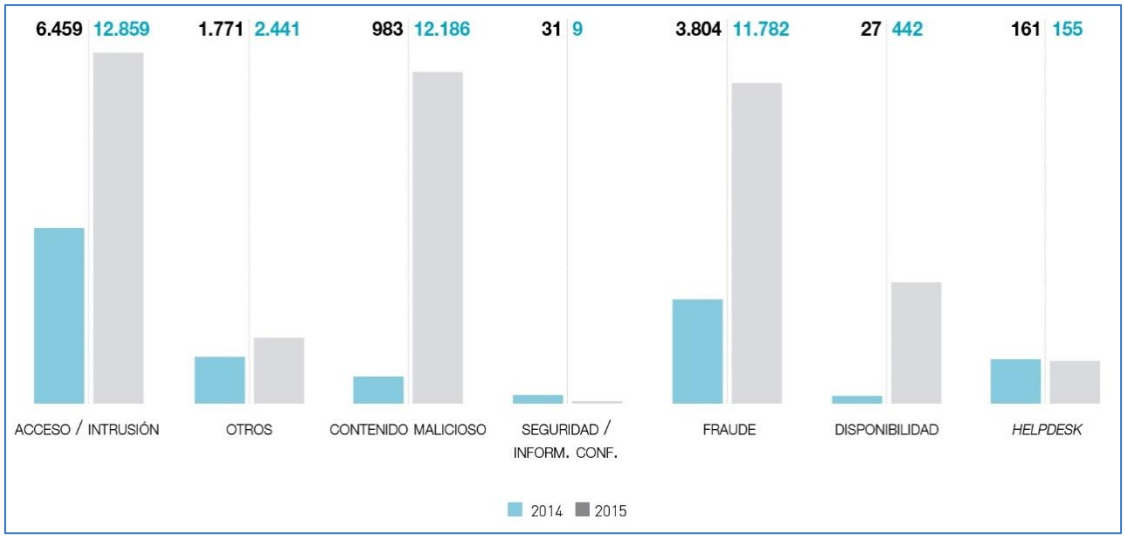


***Ilustración 30**: Informe anual de la seguridad en España: Evolución de los incidentes registrados por el CERT de seguridad e industria de INCIBE para el resto de empresas por tipología 2014-15[110].*

I.6.2.- Ultimos sucesos: Atentados de Barcelona-Cambrils

Relato de los atentados:

Todo empieza el pasado 16 de agosto del 2017 cuando sobre la 23.15 se oye un gran estruendo en una urbanización llamada Montecarlo en la población de Alcanar, provincia de Tarragona. En un primer momento se piensa en una explosión de gas y se cree que puede haber además del cadáver encontrado otro fallecido.

El chalet en cuestión está habitado por okupas, que según los vecinos son de origen magrebí y religión musulmana. En un primer momento se habla de una posible solicitud de actuación del servicio especialista de este tipo de sucesos de la Guardia Civil (TEDAX), encontrándose éstos con una negativa de los Mossos de esquadra para acceder al lugar de los hechos.

La primera determinación de lo sucedido por parte de los Mossos es errónea: No se relaciona la explosión con una posible célula terrorista,

[110] Ibídem., p. 104.

posiblemente por la falta de experiencia en este tipo de sucesos.

"La explosión que se produjo en la noche del miércoles, cuando, según todos los indicios, uno de los terroristas murió mientras preparaba una bomba que le estalló durante su elaboración, podía haber sido una prueba determinante (o al menos lo debería haber sido si se hubiera analizado correctamente) de la campaña criminal que se avecinaba.

Los citados expertos han asegurado que los Mossos d'Esquadra no comunicaron en tiempo real lo que había pasado en Alcanar a la Guardia Civil ni al Cuerpo Nacional de Policía, que se enteraron al día siguiente cuando se comunicó de forma oficial y pública lo ocurrido y se vinculó con el atentado de Barcelona.

Hubo, por lo tanto, un fallo muy importante de coordinación, ya que la explosión podía ser fortuita pero, como se ha demostrado, tenía orígenes terroristas. Tres cuerpos actuando y colaborando a la vez, con sus correspondientes bases de datos y con sus analistas, podían haber dado con la clave de que el citado piso era una base yihadista y no un local de «okupas» como se llegó a decir en los primeros momentos.

Las mismas fuentes se quejan de que la publicitada colaboración de los Mossos con la Policía y la Guardia Civil en los atentados de Cataluña deja mucho que desear y que, por ejemplo, la identificación de los terroristas muertos en el enfrentamiento de Cambrils no se había comunicado a medio día a los otros cuerpos de la Seguridad del Estado pese a que ya se tenían datos concluyentes.

«Siempre será mejor que actúen tres bases de datos a la vez que una sola. Es de una lógica aplastante», agregaron[111]. Tras lo acontecido, con toda la información y atando cabos, se detecta un mal uso de la información recibida de otros cuerpos: por un lado con toda la información facilitada por la policía belga sobre el imán de Ripoll (con antecedentes en enaltecimiento y adiestramiento de terroristastambién tuvo contacto con autores de los atentados de Bruselas, que

[111] ZULOAGA, J. M. (19 de agosto de 2017) ¿Qué pasó en Alcanar? Los Mossos no avisaron a la Guardia Civil. *La Razón*. Madrid. Recuperado de: http://www.larazon.es/espana/que-paso-en-alcanar-los-mossos-no-avisaron-a-la-guardia-civil-ON15814587

después resulto ser uno de los muertos del chalet). Además, se ha sabido que los mossos hicieron caso omiso a las recomendaciones y avisos de la CIA sobre un atentado en Barcelona para esas fechas.

El "Imán de Ripoll": ABDELBAKI ES SATTY, cerebro de los atentados de Barcelona y Cambrils, fue investigado por su presunta pertenencia a la célula de *Vilanova i La Geltrú* que lideraba MOHAMMED MRABET, gerente de la mezquita de esta localidad barcelonesa. El grupo que lideraba Mrabet en 2005 y 2006, adoctrinador de quien luego sería el imán de Ripoll, tenía varias conexiones internacionales. Las principales eran, según las investigaciones de la Guardia Civil y la Policía Nacional, con células asentadas en Marruecos, Holanda y, en menor medida, Bélgica.

Adscritos al Grupo Islámico Combatiente Marroquí (GICM), responsable del 11M, los miembros de la célula de *Vilanova* estaban conectados con el denominado «grupo de Hostahd», responsable del asesinato del cineasta holandés THEO VAN GOGH"[112].

Al día siguiente una furgoneta blanca que circulaba por la calle Pelai a las 16.50 horas, giró a la altura de Las Ramblas a una alta velocidad altamente fuera de lo normal, empezó a dar volantazos atropellando a los viandantes durante unos 600 metros, acabando con la vida de 13 personas y provocando 130 heridos. El conductor (YOUNES ABOUYAAQOUB), abandonófríamente el vehículo camuflándose en el mercado de la Boquería, siguió callejeando por El Raval, hasta llegar a la Universidad una hora y media después (18.20h), donde, tras apuñalar a un joven de Villafranca, lo dejó sin vida en la parte trasera de su vehículo, convirtiéndose en la persona asesinada número 14, tras robarle su Ford Focus para huir por la Diagonal en dirección a Tarragona.

Tras escaparse de un control atropellando a un *mosso* logra escapar y el vehículo es encontrado en *Sant Just Desvern* con el cuerpo del joven asesinado. Dos horas y media después (19.30h) del atentado, los mossos localizan un segundo vehículo, una furgoneta enfrente del Burger King en la localidad de Vic.

[112] CHICOTE, J. (4 de septiembre de 2017).El imán de Ripoll, relacionado con el atentado contra el cineasta Theo van Gogh*, ABC* España, Madrid.Recuperado de: http://www.abc.es/espana/abci-iman-ripoll-relacionado-atentado-contra-cineasta-theo-gogh-201709042148_noticia.html

Veinte minutos después (19.50h) se realizan por parte de los mossos las primeras detenciones en la población de Ripoll. Se detiene a DRISS OUKABIR SOPRANO. Este se entrega en la comisaría de los mossos al ver su imagen en los medios de comunicación, diciendo que su hermano le robó la documentación. También se detiene en esta localidad a SALH EL KARIB, dueño del locutorio donde DRISS compró el billete para supuestamente huir a Marruecos, y a MOHAMED AALLA, dueño del vehículo Audi A3 que conducían los terroristas de Cambrils. Todo el conjunto de sucesos lleva a que esa misma noche (23.00h) se relacione la explosión de Alcanar con el atropello de Barcelona a través de un comunicado de prensa de los mossos.

Ya el día 18 de agosto de 2017, pero dos horas y media después del comunicado (1.25 hs), anuncian una operación policial en la localidad costera de Cambrils. Un Audi A3 ocupado por cinco magrebís choca contra un vehículo policial de un control al lado del paseo marítimo. El vehículo atacante queda inutilizado pero los sujetos huyen por el paseo, siendo abatidos 4 de ellos por un agente. El último malhechor logró apuñalar a una mujer de mediana edad en su huida, que falleció en el centro hospitalario donde fue atendida, pasando a ser 15 las víctimas mortales del atentado. Los terroristas iban equipados con falsos cinturones de explosivos y armados con cuchillos de gran tamaño. La rápida actuación del primer mosso de escuadra exlegionario que abatió 4 yihadistas logró evitar una masacre en el paseo lleno veraneantes. El último terrorista necesitó de al menos 12 disparos de otros 2 mossos para lograr ser abatido, lo cual podría demostrar la falta de experiencia y formación de este cuerpo para este tipo de sucesos.

"Un 'mosso' adiestrado en la Legión abatió a los terroristas…"

El héroe de Cambrils, como ya se conoce al Mosso d'Esquadra que abatió a cuatro terroristas el pasado jueves tras el segundo atentado en Cataluña, fue formado durante meses en la Legión. Tras el desmentido de la Policía Autonómica, fuentes cercanas al Gobierno de España confirmaron a EL MUNDO que sí realizó el servicio militar en el Tercio Gran Capitán de la Legión, en Melilla"[113]*.*

[113] VILLARREAL, R. (24 de agosto de 2017). El 'héroe de Cambrils', instruido en Melilla. *El Mundo* Catalunya, Tarragona. Recuperado de:

Tras el segundo atentado hora y media después comparece el conseller de interior:

"Se concluye, que había una célula para atentar en *Catalunya*", según JOAQUIM FORN conseller de Interior. Se trabaja sobre la hipótesis de que este grupo estaría integrado por 12 miembros y liderado por el imán de Ripoll.

A partir de aquí, el imán de Ripoll se convierte en centro de la investigación de los atentados de Barcelona y Cambrils. Los Mossos trabajan sobre la hipótesis de que éste sería una de las dos personas halladas muertas en la explosión de Alcanar. Aparece material habitual del IS para fabricar explosivos, como acetileno y TATP y más de 120 bombonas de gas, aunque desde nuestro punto de vista esto se produce un poco tarde, ya que se le negó el acceso a los especialistas de los cuerpos del estado.

El objetivo ahora son las investigaciones policiales, centradas en hallar al conductor de la furgoneta y autor del atentado terrorista en La Rambla de Barcelona. Todos los cuerpos policiales del estado trabajan de forma conjunta para tratar de desarticular la célula terrorista.

El día 21 de Agosto de 2017 los *Mossos d'Esquadra*, gracias a la colaboración de los ciudadanos localizan a YOUNES ABOUYAAQUOUB en la población de Subirats. Es una vecina la que da el aviso. Tras verlo y preguntarle, éste huye hasta que una unidad de los Mossos lo localiza y abate tras unos disparos. De esta forma queda totalmente desintegrada la célula terrorista, aunque un poco tarde y tras la lista de 15 muertos y cientos de heridos.

Análisis del atentado:

Debemosdejar claro antes de empezar con este punto, que los únicos culpables de estos hechos son los terroristas, personas desarraigadas de sentimientos y valores humanitarios.

http://www.elmundo.es/cataluna/2017/08/24/599dec79e2704ea87f8b460b.html

No sabemos a ciencia cierta si se podrían haber evitado los atentados de Barcelona y más tarde el de Cambrils, lo que sí que es cierto es la falta de profesionalidad y descoordinación en la investigación de la explosión de Alcanar donde se dio más prioridad a ideologías políticas que a la seguridad de los ciudadanos. La unidad especializada en análisis de sucesos con explosivos (TEDAX) es una de las mejores del mundo y probablemente podría haber sacado conclusiones e ideas más concretas y profesionales pudiendo haber abortado (o no) el atentado de Barcelona pero las posibilidades de éxito de las fuerzas del orden hubieran sido más altas. Esta lucha de mando "esto es Cataluña y aquí actúan los mossos" y también el caso omiso a las recomendaciones del Ministerio de Interior (colocación de bolardos) se ha pagado cara, muy cara.

Descoordinación Policial-política:

Los sucesos posteriores a la masacre evidencian la falta de coordinación policial, y el impacto del pulso soberanista en Cataluña en la prevención e investigación de la masacre. El sindicato mayoritario en Policía (SUP) y una de las asociaciones profesionales de la Guardia Civil (AUGC), emiten un comunicado conjunto, para denunciar que a ambos cuerpos se les ha impedido servir a los ciudadanos antes, durante y después de los ataques para que la Generalitat diera «imagen» de Estado catalán autosuficiente.

¿Cómo logró un solo hombre, que además fue condenado por traficar con 121 kilos de droga y sufrió una orden de expulsión de España, reclutar y convencer a otros 11, regatear a las fuerzas del orden, esquivar una investigación como fue la *operación Chacal*, viajar por Europa propagando su discurso de odio, localizar y *okupar* un chalet en Cambrils, hacerse con un centenar de bombonas de butano y media tonelada de acetona, y todo ello siendo indetectable?

Un policía belga pregunta por ES SATTY, mediante un simple correo electrónico, a un *mosso d'esquadra* amigo que había conocido en un encuentro policial europeo. El responsable de los Mossosmira y no halla nada en sus bases. Curiosamente le sale otro ES SATTY de la *operación Chacal*, MOSTAPHA, exonerado. El *mosso* contesta que no tiene información y las andanzas por Europa de ES SATTY, en ese momento ya radicalizado o bien radicalizándose, quedan

fuera del radar policial una vez más[114].

Los bolardos:

Tras el atentado que dejó 85 muertos en Niza en el verano de 2016, el Ayuntamiento de Barcelona se negó repetídamente, pese a las recomendaciones del Ministerio de Interior y del propio Departamento de esa área de la Generalitat, a instalar barreras físicas de protección para la eventualidad de posibles atentados con vehículos motorizados. Según se ha informado, el Consistorio apostó por la presencia policial constante en los lugares más sensibles en este aspecto en la ciudad, pese a que desde hacía años La Rambla y la Sagrada Familia aparecían constantemente entre los escenarios más plausibles para que el Estado Islámico lograra la mayor difusión posible para sus atentados[115].

"Aviso de la CIA y de la Policía Nacional":

Un nuevo eslabón en la cadena de fallos: los Mossos d'Esquadra recibieron la alerta por parte de la CIA del atentado de La Rambla el 25 de mayo, en un aviso también remitido al Cuerpo Nacional de Policía y la Guardia Civil.

Según la información adelantada por *El Periódico de Catalunya*, los servicios de inteligencia de Estados Unidos contactaron con la policía para alertarles de un atentado inminente que iba a orquestar el Estado Islámico en verano en la ciudad.

Fuentes de las lucha antiterroristas confirmaron a EL MUNDO que esta información es "impecable" y que la Policía dio traslado de ese aviso a los Mossos en la semana del 25 de mayo"[116].

La juez:

Una cantidad inesperada de bombonas de butano provocó las dudas de la juez de Amposta (Tarragona) que investigó en la noche del miércoles 16 de agosto, sólo horas antes de los atentados, sobre la versión que manejaban *los*

[114] ALSEDO, Q. Y HERRÁIZ, P. (31 de agosto de 2017). Sombras y errores de la investigación de los atentados de Barcelona y Cambrils*. El Mundo, Madrid.* Recuperado de: http://www.elmundo.es/cataluna/2017/08/25/599f2c56e5fdeab0598b4641.html

[115] Ibídem.

[116] Ibídem.

Mossos: que lo que acababa de explotar era un laboratorio de droga. Dos nuevos estallidos, ya de noche, hicieron dudar aún más a la magistrada. El cuerpo policial catalán de hecho sólo localizó un cadáver en aquel momento, pero halló restos de otros tres cadáveres cuando emergió la verdad: que allí no se preparaba droga para vender, sino bombas para causar cientos de muertos en monumentos como la Sagrada Familia, como ha declarado uno de los yihadistas, MOHAMED HOULI, ante el juez FERNANDO ANDREU. Los Mossos no dejaron a la Guardia Civil actuar, pese a la experiencia de la Benemérita.

«El explosivo habría resultado llamativo a nuestros TEDAX», dijo un responsable dela AUGC (Asociación Unificada de la Guardia Civil)[117].

No se utilizó toda la experiencia de nuestros cuerpos de seguridad, unos cuerpos altamente formados con un prestigio altísimo a nivel internacional y que son el orgullo de nuestra nación, que por desgracia cuentan con una experiencia en terrorismo de muchas décadas de lucha contra ETA y GRAPO siendo ejemplo y formación de muchos otros cuerpos de países amigos que se encuentran con un problema y cuestiones nuevas con acciones terroristas que a veces desbordan la seguridad de los países.

La impresión (después de analizar los datos de este atentado), es que, sin desprestigiar a los Mossos en ningún momento, ya que éstos realizan con nota de sobresaliente la gran mayoría de tareas encomendadas, como policía urbana, de tráfico, judicial etc., es que hay ciertas tareas que requieren de una más alta especialización, medios y dirección como es el caso de los sucesos de índole terrorista en los cuales la premisa rapidez puede decantar la balanza al lado de la ley en muchos sucesos, evitando de esta forma matanzas y aunque nunca diremos que ésta se hubiera podido evitar, sí que podemos afirmar que las diligencias realizadas no se han hecho con la extrema celeridad y rapidez exigibles en estas circunstancias.

[117] Ibídem.

CAPÍTULO II

VISIÓN INTERNACIONAL DE LA CIBERSEGURIDAD

Y EL CIBERTERRORISMO

II.1.- ANÁLISIS GENERAL INTERNACIONAL

España como estado dentro de la UE y perteneciente a la OTAN forma parte del sitema defensivo de ambas y dispone de tecnología capaz, para desarrollar su labor como tal, además esta obligada a cumplir con las normativas y directrices de seguridad que de estas se derivan, esto nos permite formar parte de las naciones con estrategias defensivas desarrolladas y capaces de evitar y contrarrestar los posibles ataques a los que como parte del ciberespacio estamos expuestos.

Aún hay muchos países muy vulnerables ante el hecho de que un *hacker* profesional con ganas de pasar «un buen rato» les juegue una mala pasada: «Según GILMA, un hacker de origen hindú, las posibilidades de que dispones una vez que has accedido a un ordenador ajeno son infinitas. A mí me sería posible hackear una máquina paquistaní y, por medio de un sencillo programa, hacer que desde ese sistema se lanzase un ataque a varios servidores de Estados Unidos, haciéndoles creer que el responsable es el propietario del ordenador en el que he entrado, y provocando quizá un ambiente de tensión entre los dos países» (VÁZQUEZ LIÑÁN, 2000).

En el caso de la guerra en Chechenia analizado por VÁZQUEZ (2000) los ataques cibernéticos han sido contínuos por parte de ambos bandos. Los hackers rusos, de gran «prestigio» internacional, intercambian mensajes cifrados a través

de diferentes sitios web para organizar su «guerra». Son múltiples las armas quese pueden usar en este tipo de guerra. Todo el que tenga un ordenador personal con conexión a Internet posee el laboratorio para crearlas y, dependiendo de su pericia y conocimientos, puede tener en casa desde una simple navaja al arma más sofisticada y destructiva: términos como *troyano* (programa que se introduce y apodera de ordenadores ajenos), *sniffer* (aplicación que se introduce en sistemas previamente hackeados para interceptar información en tránsito), *i-worms*, módulos maestros, etc., son sólo algunos de los cientos que definen esta clase de armas. La propuesta central que llevó EE.UU. a esta cumbre del G-8 fue la creación de una ciberpolicía internacional, algo que ya existe, pero que sin un acuerdo a nivel mundial (ya sabemos lo difícil que es esto), sólo puede ser parcial y con muchas fisuras. El origen del virus "*I Love you*" fue localizado en Filipinas, lo que puso a muchos en guardia acerca de la necesidad de cooperación internacional en este tipo de delitos.

La Unión Europea (UE) ha desarrollado unos instrumentos Jurídicos para luchar contra el Ciberterrorismo, unos instrumentos que llegan de un lado al otro de sus fronteras y cuyo principal cometido es la estandarización de las legislaciones de todos sus miembros para luchar de forma efectiva contra los ciberdelincuentes.

El objetivo no es estudiar los aspectos militares o los discursos políticos sobre Internet en los Estados miembros. La meta es presentar el papel de la Unión Europea en la consecución del ciberespacio como un espacio de libertad, seguridad y justicia. "Tomando en consideración que gran parte de la vida de los ciudadanos se realiza conectada a Internet, no nos encontramos ante un problema superfluo. El siguiente paso del trabajo, una vez presentados cuáles son los usos terroristas *de facto* en Internet, es ineludible: identificar y analizar los instrumentos en materia de seguridad civil que pueden ser empleados en esta batalla global, así como las propuestas de mejora al respecto. Una de las principales vías para combatir el ciberterrorismo y aumentar la seguridad en Internet es armonizar las leyes nacionales. Este método permitiría en principio reducir la impunidad y evitar desigualdades en la prevención y persecución según el Estado donde se produzca el acto. En este campo, la UE goza de un papel protagonista dado que entre sus competencias figura la de adoptar normas mínimas y armonizar leyes penales

nacionales, si bien está sujeta a unas estrictas limitaciones" (SÁNCHEZ FRÍAS, 2016).

Un ejemplo práctico: LA GUERRA DE KOSOVO. Si ya la Guerra del Golfo fue un conflicto espectacularmente mediatizado, con batallas en horas de máxima audiencia y enormes tarifas de inserción publicitaria durante su retransmisión televisiva, a la ex Yugoslavia le ha tocado el triste privilegio de ser la primera guerra en la que Internet ha jugado un importante papel. Ocurrió en Bosnia-Herzegovina, y de forma mucho más clara en Kosovo. Miles de periodistas de todo el mundo, además de todo el que estuviese interesado en el conflicto, pudieron seguir a través de toneladas de información, la guerra de Kosovo a través de Internet. Y no nos estamos refiriendo a la cobertura que los grandes medios y grupos de comunicación del mundo dieron sobre el conflicto, sino a cientos de webs que surgieron para, desde todos los puntos de vista, aportar información y propaganda sobre la guerra. Muchos de ellos siguen en activo, algunos incluso actualizando su información a diario. La versión oficial del gobierno serbio estaba en *www.kosovo.com*, y en otros sitios como *Mediacentar Pristina*, a cargo de un supuesto «Centro de medios de Pristina». Aquí se podían encontrar versiones con comentarios sobre el terrorismo kosovar, limpieza étnica llevada a cabo por los kosovares, leyes yugoslavas que protegen a las minorías étnicas, etc. Del otro lado, es especialmente interesante la historia de la emisora de radio independiente de Belgrado B-92 *(www.b92.net),* que se convirtió en todo un símbolo porque, tras sufrir la persecución y censura del gobierno de SLOBODAN MILOSEVIC, siguió transmitiendo a través de la Red en *Real Audio*, hasta que la policía la clausuró por la fuerza. Este hecho hizo que surgieran multitud de webs en apoyo de B-92. El Ministerio de Defensa británico tradujo al serbio la web de la institución, «para que los que tengan computadoras personales puedan saber la verdad acerca de MILOSEVIC y su brutal represión. De las 150.000 visitas de la *web site* diarias, 1.400 son desde Yugoslavia». La solidaridad rusa con el hermano serbio llevó al ataque, por parte de los hackers rusos al sitio de la OTAN. Estos piratas informáticos declararon la guerra a la Alianza Atlántica en el nodo *www.hackzone.ru,* en el que se daban cita los hackers para coordinar su estrategia de ataque y recibir instrucciones, poniendo en jaque en varias ocasiones al servidor de la mismísima Casa Blanca. Kosovo fue el principio, pero muchos conflictos posteriores han

seguido el ejemplo. La guerra palestino-israelí también se ha llevado a Internet, a través de sitios que, una vez más, se han enzarzado en una guerra informativa.

Según ACURIO DEL PINO (2011), "El primer acercamiento a las acciones delictivas informáticas debe considerarse en primer términoen 1983. LaOCDE inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales. Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración *iuscomparativista* de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena. De esta forma, la OCDE en 1986 publicó un informe titulado "Delitos de Informática: análisis de la normativa jurídica", en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales"[118].

A continuación veremos algunas decisiones Jurídicas tomadas en diferentes países para la defensa contra el ciberdelito y su estrategia de ciberseguridad (ver Anexo II):

a) Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los

[118] ACURIO DEL PINO, A. (2011). Delitos informáticos: Generalidades. (OEA) Jurídica Cono Sur. Recuperado de : http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

siguientes delitos[119]:

- Espionaje de datos (piratería informática, art. 202a.
- Estafa informática (art. 263a).
- Falsificación de datos probatorios (art. 269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica y uso de documentos falsos (art. 270-273).
- Alteración de datos. Es ilícito cancelar, inutilizar o alterar datos. Incluso la tentativa es punible (art. 303a).
- Sabotaje informático. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa (art 303b).
- Utilización abusiva de cheques o tarjetas de crédito (art 266b).

Alemania publicó en 2011 su estrategia de ciberseguriadad (*Cyber Security Strategy for Germany*)[120] y actualizó su legislación sobre información tecnológica en julio de 2015, con la aprobación de la Ley alemana de seguridad informática ("*IT-Sicherheitsgesetz*"). La Ley de Seguridad Informática modificó una serie de leyes existentes e introdujo las obligaciones de seguridad y notificación de TI, principalmente para varios de los llamados "Operadores de Infraestructura Crítica" que prestan servicios de interés general. En julio de 2016, la Directiva sobre Seguridad de Redes y Sistemas de Información ("Directiva NIS *Network and Information Systems*") fue aprobada por el Parlamento Europeo. Para abril de 2018, los Estados miembros de la UE deben transponer las disposiciones de la Directiva NIS a las leyes nacionales. En consecuencia, en abril de 2017, Alemania aprobó la Ley de Implementación de la Directiva NIS ("NIS-

[119] Vid. Deutsches Strafgesetzbuch (Código Penal Alemán) Recuperado de: https://www.gesetze-im-internet.de/stgb/

[120] FEDERAL MINISTRY OF THE INTERIOR, GERMANY. (2011). Cyber Security Strategy for Germany. Recuperado de: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Umsetzungsgesetz")[121].

b) Austria

Ley de reforma CP de 22 de diciembre de 1987. Esta ley contempla los siguientes delitos[122]:

- Destrucción de datos (corrupción de datos art. 126a, fallo Sistema informático art. 126b, acceso a programas informáticos art. 126c). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

- Estafa informática (art. 148a). En este artículo se sanciona a aquellos que con *dolo* causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes cometen este hecho utilizando su profesión.

Además, Austria publicó en 2012 la National ICT Security Strategy, y en 2013 su estrategia de seguridad (Austrian Security Strategy) y la estrategia de ciberseguridad (Austrian Cyber Security Strategy)[123].

c) Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático[124]:

[121] WESSING, T. (16 de agosto de 2017). The German IT Security Law. Lexology. Recuperado de: https://www.lexology.com/library/detail.aspx?g=9368f280-b504-4914-8850-30ca58774e00

[122] Vid Strafgesetzbuch Österreich (Código Penal de Austria). Recuperado de: https://www.jusline.at/gesetz/stgb/paragraf/126

[123] Vid. National ICT Security Strategy <https://www.digitales.oesterreich.gv.at/documents/22124/30428/National_ICT_Security_Strategy_Austria_2012_print.pdf> Vid. Austrian Security Strategy <http://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf>. Vid. Austrian Cyber Security Strategy < http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50999 >

[124] Vid. Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique (Legislación informática Francia). Recuperdo de: http://www.informatica-juridica.com/anexos/legislacion-informatica-de-francia-loi-no-88-19-du-5-janvier-1988-relative-a-la-fraude-informatique/

- Acceso fraudulento a un sistema de elaboración de datos (art. 462.2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

- Sabotajeinformático. El art. 462.3 sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

- Destrucción de datos. Artículo 462.4 sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.

- Falsificación de documentos informatizados (art. 462.5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

- Uso de documentos informatizados falsos (art. 462.6). Se sanciona a quien conscientemente haga uso de documentos falsos.

Por otra parte, Francia publicó en 2015 su estrategia de ciberseguridad (*French National Cyber Security Strategy*) en la que marca cinco objetivos: 1) Intereses fundamentals, defense y seguridad de los sistemas de información del Estado y de las infraestructuras críticas, crisis informática mayor; 2) Confianza digital, vida privada, datos personales, ciberataques; 3) Sensibilización, formaciones iniciales, formaciones continuas; 4) Entorno de las empresas del sector digital, política industrial, exportación e internacionalización; 5) Europa, soberanía digital, estabilidad del ciberespacio[125].

[125] Vid. *French National Cyber Security Strategy* 2015. Recuperado de: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy

d) Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986[126].

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etcétera y en qué difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión. Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él sólo quería enviar un mensaje[127].

La Administación de Estados Unidos publicó en diciembre de 2017 su estrategia nacional (*National Security Strategy of the United States of America*)[128]. Además en materia de ciberseguridad, tiene los siguientes documentos[129]:

- *The Department of Defence Cyber Strategy* (2015).
- *Cybersecurity Act of* 2015.

[126] ACURIO DEL PINO, A. (2011). Ob., cit., pp 36-37.
[127] Ibídem.
[128] Vid. National Security Strategy of the United States of America (2017) Recuperado de: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[129] Vid. documentosCiberseguridad Estados Unidos. Recuperado de: https://ccdcoe.org/cyber-security-strategy-documents.html

- *Cybersecurity Enhancement Act of* 2014.
- *National Cybersecurity Protection Act of* 2014.
- *Draft Strategy for Improving Critical Infrastructure Cybersecurity* (2014).
- *President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity* (2013).
- *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (2011).
- *Cyberspace Policy Review* (2009).
- *The National Strategy to Secure Cyberspace* (2003).

e) Chile

En junio de 1993 entró en vigencia en Chile la Ley n° 19.223, sobre delitos informáticos. La Ley nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: "la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan". La Ley n° 19.223, es una ley especial, extra código y consta de 4 artículos, que se enuncian a continuación[130]:

Artículo 1. "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Artículo 2. "El que, con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a

[130] ACURIO DEL PINO, A. (2011). Ob., cit., p 38.

medio".

Artículo 3. "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

Artículo 4. "El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

En la Ley nº. 19.223 se contemplarían los delitos informáticos de sabotaje y espionaje informáticos, aunque no de una forma clara. Así, en el artículo 1, el inciso primero alude a los daños que se puedan cometer contra el hardware, sea destruyéndolo o inutilizándolo, por lo que no se trataría de un delito informático sino más bien de un delito de daños convencional. Es el artículo 3° donde encontraríamos la figura del sabotaje informático al sancionar al que maliciosamente altere, dañe o destruya los datos contenidos en un sistema.

Por otra parte, en abril de 2015, Chile presentó la "Política Nacional de Ciberseguridad"[131], que cuenta con cinco objetivos estratégicos:1) contar con una infraestructura de la información capaz de resistir y recuperarse en caso de ataques e incidentes de ciberseguridad; 2) velar por los derechos de las personas en el ciberespacio; 3) desarrollar en Chile una cultura de la ciberseguridad, que contemple no sólo a los actores públicos y empresariales, sino también a los ciudadanos y ciudadanas respecto de las prácticas digitales; 4) avanzar en conjunto con los organismos internacionales y "nuestros países amigos en los desafíos", 5), promover el desarrollo de una industria de la ciberseguridad, que permita posicionar a Chile de mejor manera en la región, aprovechando las ventajas estratégicas[132].

[131] MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA, CHILE (2017). Política Nacional de Ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

[132] SUBSECRETARÍA DE DEFENSA, CHILE. (27 de abril de 2017). Una Política de Ciberseguridad para Chile. Recuperado de: http://www.ssdefensa.cl/n5427_27-04-2017.html

II.2.- COOPERACIÓN HISPANO-MARROQUÍ EN MATERIA ANTITERRORISTA

Es Marruecos por su situación sobre todo geográfica, estratégica y históricamente el país del mediterraneo Africano, que mas relación tiene en estos momentos con España, es también el país de origen de casi la totalidad de inmigrantes musulmanes establecidos en nuestras fronteras y por supuesto foco y cuna de los terroristas islámicos que han sido detenidos en España. Todo ello nos hace formular un gran interés por el estudio y análisis en cuanto a terrorismo y Marruecos se refiere.

II.2.1.-Código Penal de Marruecos

Estudio general del CP antiterrorista marroquí:

- El Código Penal marroquí es del 5 de junio de 1963.
- En 2015 se creó la nueva ley marroquí en materia antiterrorista.
- A pesar de que las sentencias serán revisadas a la baja, la Corte Penal Antiterrorista marroquí va a expandir el ámbito de hechos punibles contra el terrorismo yihadista.

II.2.2.-Nueva Ley antiterrorista de Marruecos

- El proyecto de ley fue presentado a finales de octubre del 2015 por el ministro de Justicia marroquí, MUSTAPHA RAMID y se contempló que el sustento del cuerpo legal en materia antiterrorista se orientará por reglas claramente proactivas.
- El futuro texto legal contiene disposiciones que prevén la anticipación al hecho terrorista.
- En términos CP, la lista de actos considerados terroristas se extiende. De hecho, incluye unir o tratar de unir de forma individual o colectiva, en un entorno organizado o no, a las estructuras, asociaciones o grupos terroristas, independientemente de su forma, objeto o lugar, aunque los hechos no afecten al Reino de Marruecos o sus intereses.

- El proyecto de ley también se ocupa de los campamentos de entrenamiento de terroristas, dentro o fuera del territorio marroquí, con el fin de cometer actos terroristas en Marruecos o en el extranjero, se produzca o no el acto en sí.
- Igualmente se penará la publicidad, la tolerancia o la promoción de entidades o grupos terroristas, independientemente del soporte en el que se produzca: escritos, impresos distribuidos o comercializados o mostrados en reuniones o lugares públicos o mediante carteles expuestos a la vista del público. Los actos anteriores podian ser castigados con penas de prisión de cinco a diez años y multa de 5.000 a 10.000 dirhams[133]. A partir de ley del 2015 se modifica a penas de cinco a 15 años de prisión y multa de hasta 500.000 dirhams.
- Retirada de pasaporte. Uno de los parámetros a tener en cuenta en la nueva ley es la confiscación de pasaportes de ciudadanos marroquíes sospechosos de pertenecer a organizaciones terroristas relacionadas con la yihad, lo que repercutiría en dificultar su entrada en Ceuta y Melilla a través de los tránsitos normales en las fronteras.
- La Fiscalía General Pública de la Corte de Apelaciones tiene derecho, cuando se trata de un delito de terrorismo, a retirar el pasaporte de los acusados y personas cercanas a ellos por un período de seis meses renovables una sola vez. Este plazo podrá ser prorrogado hasta el final de la audiencia preliminar si es la causa de la demora.

Ley antiterrorista Marroquí 2015

A continuación veremos algunos artículos del Proyecto 86,14, ley que modifica y completa el Código Penal y los procedimientos penales relativos a la lucha contra el terrorismo en Marruecos.

Artículo primero: Las disposiciones del capítulo I bis del Título I del Libro III CP aprobado por el Dahir nº 1-59-413, de 28 Jumada II 1382 (26 de noviembre 1962) se complementan de la siguiente manera: Artículo 218-1-1: Constituyen

[133] El dirham درهم es la moneda oficial del Reino de Marruecos. 1 EUR = 11,1278 MAD (mayo de 2018).

delitos de terrorismo los actos siguientes:

- Reunir o intentar reunir individual o colectivamente dentro de un marco organizado o no organizado a entidades terroristas, organizaciones, bandas o grupos, cualquiera que sea su forma, su objeto, o el lugar donde se encuentran, incluso si los actos los terroristas no pretenden perjudicar al Reino de Marruecos ni a sus intereses.

- Recibir o intentar recibir capacitación o formación en cualquier forma, naturaleza o duración dentro o fuera del territorio del Reino de Marruecos, con el fin de cometer un acto de terrorismo dentro o fuera del reino independientemente de la ocurrencia de tal acto.

- Alistar, entrenar o intentar reclutar o capacitar a una o más personas, con miras a su unión a entidades, organizaciones, bandas o grupos, terroristas dentro o fuera del territorio del Reino de Marruecos.

Los actos mencionados son punibles con pena de prisión de cinco a quince años y una "multa" de 50.000 a 500.000 dirhams. Sin embargo, cuando el delincuente es una persona pública, será castigado con una multa de 250.000 a 2.500.000 dirham, pronunciándose contra la disolución y las dos medidas de seguridad previstas en el Artículo 62 del presente Código, sujeto a los derechos de terceros y sin perjuicio de sanciones que puedan imponerse a líderes o agentes que hayan cometido o hayan intentado cometer el delito.

Artículo 2. Las disposiciones del artículo 218-2 del mencionado Código Penal son complementadas con el párrafo siguiente. Artículo 218-2 (párrafo segundo): Toda persona que, por uno de los medios previstos en el párrafo primero de este artículo, realice propaganda, apología o promoción de entidades, organizaciones, bandas o grupos terroristas, será castigada con la misma pena.

Artículo 3. Se modifican las disposiciones del artículo 218-5 del citado Código Penal como sigue. Artículo 218-5: Quien por cualquier medio persuada, incite o provoque a otra persona para cometer cualquiera de los delitos previstos en este capítulo, será castigado con pena de prisión de cinco a quince años y multa de 50.000 a 500.000 dirhams.

Artículo 4. Las disposiciones del título II del libro Vil de la Ley n ° 22.01 sobre el procedimiento penal promulgado por el dahir n ° 1.02.255 de 25 - 1423 (3 de octubre de 2002) se completan como sigue: Artículo 711-1: Sin perjuicio de cualquier disposición estatutaria en contra, serán procesados y juzgados ante los tribunales marroquíes competentes a cualquier ciudadano marroquí o extranjero que haya cometido como autor, coautor o cómplice, "un delito terrorista, teniendo o no la intención de perjudicar al Reino de Marruecos o sus intereses".

No obstante, cuando los actos de terrorismo no tengan por objeto perjudicar al Reino de Marruecos o sus intereses y cuando se cometan fuera del territorio del Reino por un extranjero como autor, coautor o cómplice, puede ser procesado y juzgado de conformidad con las disposiciones de la ley marroquí sólo si se encuentra en el territorio nacional.

La acusación o juicio del acusado no puede tener lugar si demuestra que ha sido juzgado en el extranjero por el mismo hecho por una decisión que ha adquirido fuerza de cosa juzgada y, en caso de convicción, haber sufrido su sentencia o si justifica el plazo de prescripción.

II.2.3.-Cooperación policial y judicial antiterrorista entre España y Marruecos

"Los recientes atentados de Bruselas[134] han vuelto a poner de manifiesto la importancia de la coordinación entre países en la lucha contra el terrorismo. La colaboración judicial y policial de España y Marruecos en esta batalla es un ejemplo claro: ha permitido la desarticulación de numerosas células integristas e impedido el reclutamiento de nuevos adeptos para el DAESH. El 24 de agosto de 2015, agentes de las Fuerzas y Cuerpos de Seguridad españoles y de los servicios de Inteligencia marroquíes, la Dirección General de Supervisión del Territorio (DGST), desarticularon una red de 14 presuntos integristas que pretendían atentar

[134] Vid. Noticia El Mundo: "Una ola de explosiones ha sacudido Bruselas a primera hora del 22 de marzo de 2016, que se han cobrado al menos 31 vidas y han dejado alrededor de dos centenares de heridos, cuatro de ellos españoles. Dos detonaciones han tenido lugar en el aeropuerto Zaventem de la capital belga y una tercera se ha registrado en la estación de metro de Maelbeek, situada en la calle de la Loi, cerca del edificio de la Comisión Europea". Recuperado de: http://www.elmundo.es/internacional/2016/03/22/56f0f2cf22601d20498b4648.html

en ambos países[135]."

España lleva diez años utilizando esta estrategia de cooperación hispano-marroquí, desarticulando células para evitar atentados y envío de combatientes del DAESH. Esta estrategia fue presentada en Europa por España como modelo de referencia siendo reconocido su éxito y eficacia por GILLES DE KERCHOVE, coordinador antiterrorista de la UE[136].

"La colaboración entre España y Marruecos se inició en los años 80 del pasado siglo, pero no fue hasta la década del 2000 cuando se intensificó y amplió de manera significativa tras el atentado de Casablanca en mayo de 2003, y sobre todo, tras la masacre del 11 de marzo de 2004 en Madrid. Entre las primeras iniciativas tomadas por los gobiernos de España y Marruecos para mejorar su colaboración judicial, ámbito que ha jugado un papel clave en los buenos resultados obtenidos en la lucha contra el terrorismo yihadista, figura la designación en septiembre de 2004 de magistrados de enlace, cuya labor es la de facilitar una relación judicial más fluida y rápida entre ambos estados. España y Marruecos forman parte además, junto con Francia y Bélgica, del Grupo Cuatripartito de Fiscalías Antiterroristas**,** cuyo objetivo es también el intercambio de información sobre las investigaciones que lleva a cabo cada país**.** Esta cooperación ha permitido impedir atentados y desarticular células afines al DAESH. Nuestro país también colabora con las principales agencias y servicios antiterroristas occidentales, con el fin de investigar cualquier actividad en territorio español de integristas detectados en Europa"[137].

Los más prácticos y prestigiosos entendidos de la lucha antiterrorista internacional y más concretamente en España, convergen en la idea de que si se produce un mayor estímulo en la lucha antiterrorista de origen yihadista dentro de las fronteras marroquís esto repercutirá de forma positiva en el éxito para el control del fenómeno en Europa y concretamente en España.

[135] MARCA ESPAÑA. (7 de abril de 2016). Cooperación hispano-marroquí contra el terrorismo, un modelo a seguir. *www.marcaespaña.es*. España. Recuperado de*:* http://marcaespana.es/actualidad/cooperaci%C3%B3n-hispano-marroqu%C3%AD-contra-el-terrorismo-un-modelo-seguir

[136] Ibídem.

[137] Ibídem.

Tal como detalla en su artículo el Magistrado encargado del enlace entre ambos países D. ÁNGEL LLORENTE publicadoel pasado 20 de diciembre de 2010 en el portal web del Real Instituto El Cano:

"La cooperación judicial hispano-marroquí constituye un factor clave en la lucha contra el terrorismo internacional, como se demostró tras los atentados del 11-M. **Resumen**: Marruecos y España son dos países vecinos que están obligados a entenderse porque se necesitan mútuamente. Mantener unas buenas relaciones de vecindad es presupuesto de una acción exterior responsable e inteligente, especialmente cuando existen importantes intereses que afectan a la seguridad. La cooperación bilateral ha experimentado un creciente desarrollo en casi todos los sectores, influenciada por el fenómeno de la globalización y por la aproximación de Marruecos a Europa. Existía, no obstante, una laguna en el sector de la Justicia, que las dificultades de interlocución surgidas al inicio de la investigación de la trama marroquí en el 11-M dejaron al descubierto. Puede decirse que en la cooperación judicial hispano-marroquí hay un antes y un después del 11 de marzo de 2004. A raíz de los atentados terroristas se puso en marcha una estrategia conjunta que ha abierto los canales de comunicación necesarios para el establecimiento de una eficaz colaboración. Este modelo puede ser una referencia para el análisis, en la medida que ejemplifica las posibilidades de cooperación entre países europeos y árabes en un ámbito tan crucial como necesario"[138].

Es evidente que no basta con crear una estrategia de lucha antiterrorista a nivel nacional, europeo o incluso del mundo Occidental. Es necesario implementar esta estrategia con los países del tercer mundo y sobre todo con aquellos países de ideología musulmana que puedan tener una posible proyección yihadista, formándolos, subvencionándolos y ayudándoles a implementar una posible estrategia conjunta y operativa coherente, práctica y de posible éxito.

[138] LLORENTE, A. (20 de diciembre de 2010). La cooperación judicial antiterrorista entre España y Marruecos. ARI, Real Instituto El Cano, España. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari174-2010

Un prueba de esta colaboración es el congreso realizado en Madrid el pasado 15-06-2017 "*New Approaches on Fighting Security threats*" [139], donde se reunieron países europeos, países del Este, Orientales, Magreb etc., en el que éstos primeros han intentado trasladar a los menos desarrollados sus estrategias de lucha antiterrorista y para poderles aclarar posibles dudas pero sobre todo tener una toma de contacto entre profesionales y para de esta forma abrir las puertas a una posible colaboración entre países buscando conseguir éxito en la lucha antiterrorista[140].

II.3.- PORTUGAL, LEGISLACIÓN ANTITERRORISTA Y COOPERACIÓN INTERNACIONAL

Las leyes portuguesas, como todas las leyes de los países miembros de la UE, han sufrido recientes actualizaciones. En la entrevista al profesor FONTES[141] comenta acerca de las constituciones de los países miembros de la Unión Europea incluyendo Portugal. Según su opinión "todas las constituciones se han actualizado o deben actualizarse a los momentos actuales con la aparición del mundo digital". El citado profesor, no está en contra del desarrollo de una constitución europea pero piensa que no será una tarea fácil constituirla. Mientras, es indispensable estandarizar las leyes y en particular las antiterroristas fomentando la cooperación internacional, en el ámbito de la información, siendo probablemente necesaria la creación de una ley europea de seguridad antiterrorista cibernética"[142].

[139] El Centro Universitario de la Guardia Civil (CUGC) organizó el Congreso Internacional "Innovaciones tecnológicas y legales en la UE contra las amenazas a la seguridad" en colaboración con la Comisión Europea en el desarrollo de proyectos de fortalecimiento institucional y estabilidad en nuestras fronteras exteriores y otros escenarios geopolíticos, con el objetivo de romover el conocimiento de experiencias del Espacio Europeo de Educación Superior (EEES) en materia de tecnología y seguridad, en las fronteras exteriores de la UE. Vid. Más información en: https://www.cugc.es/extension-universitaria/actividad-internacional/item/36-innovaciones-tecnologicas-taiex-2017

[140] Vid. Apartado II.6.4 de esta investigación.

[141] FONTES, J. (2018). Professor associado com agregaçao, *Observatorio Político*. Recuperado de: http://www.observatoriopolitico.pt/jose-fontes

[142] Entrevista al profesor JOSÉ FONTES por PONS GAMÓN. Academia Militar Portuguesa (2018), prácticas de movilidad, realizadas en el marco del programa internacional.

II.3.1.- Ley antiterrorista Portuguesa

Portugal, como país miembro de la UE sigue con la línea de estandarización y convergencia europea de las leyes y en este caso concreto de las leyes Penales antiterroristas.

La ley antiterrorista portuguesa[143], fue creada en 2003 y a partir de aquí ha sufrido diferentes actualizaciones (2007, 2008, 2011, 2015), la última de ellas, al igual que la ley española y la marroquí data de 2015. Los artículos modificados y sus puntos, son los siguientes:

"Ley nº 60/2015, de 24 de junio.

Cuarta modificación de la Ley nº 52/2003, de 22 de agosto (Ley de lucha contra el terrorismo), criminalizando la apología pública y los desplazamientos para la práctica del crimen de terrorismo.

La Asamblea de la República portuguesa decreta, de conformidad con la letra c) del artículo 161 CE, lo siguiente:

Artículo 1. Objeto. La presente ley procede a la cuarta modificación de la Ley nº 52/2003, de 22 de agosto (Ley de lucha contra el terrorismo), criminalizando la apología pública y los desplazamientos para la práctica del crimen de terrorismo.

Artículo 2. Modificación de la Ley nº 52/2003, de 22 de agosto. Los artículos 4, 5 y 5 bis de la Ley nº 52/2003, de 22 de agosto, modificada por las Leyes n ° 59/2007, de 4 de septiembre, 25/2008, de 5 de junio, y 17/2011, del 3 de mayo, pasan a tener la siguiente redacción:

Artículo 4. Punto 2 - Quien comete delito de robo cualificado, robo, extorsión, burla informática y en las comunicaciones, falsedad informática, o falsificación de documento para la comisión de los hechos previstos en el apartado 1 del artículo 2, se castiga con la pena correspondiente al crimen practicado, agravado de un tercio en sus límites mínimo y máximo.

[143] MINISTERIO PÚBLICO. PORTUGAL. (2003). PGDL (Procuradoria-Geral distrital de Lisboa), Lei nº 52/2003 de 22 de Agosto, nueva ley de combate o terrorismo. Recuperado de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=119&tabela=leis&so_miolo=

Punto 4. Cuando los hechos previstos en el apartado anterior sean practicados por medio de comunicación electrónica, accesibles por Internet, el agente es castigado con pena de prisión de 1 a 6 años.

Punto 5 - Quien, con el propósito de ser reclutado para la práctica de los hechos previstos en el apartado 1 del artículo 2, con la intención en él referida, acceder o obtener acceso, a través de sistema informático o por cualquier otro medio, a los mensajes aludidos en el apartado 3 y de ellas hace uso en la práctica de los respectos actos preparatorios, es castigado con pena de prisión hasta 3 años o multa hasta 360 días.

Punto 8 - Quien, en reunión pública, a través de medios de comunicación social, por difusión de escrito u otro medio de reproducción técnica, pretenda recompensar o alabar a otra persona, grupo, organización o asociación por la práctica de los hechos previstos en el apartado 1 del artículo 2, de forma dirigida a crear peligro de la práctica de otro crimen de la misma especie, es castigado con pena de prisión hasta 3 años o con pena de multa hasta 360 días.

Punto 9 - Cuando los hechos previstos en el apartado anterior sean practicados por medios de comunicación electrónica, accesibles por Internet, el agente es castigado con pena de prisión hasta 4 años o con pena de multa hasta 480 días.

Punto 10 - Quien, por cualquier medio, viaje o intente viajar a un territorio distinto de su Estado de residencia o nacionalidad, con el fin de entrenar, dar apoyo logístico o instrucción de otro para la práctica de hechos previstos en el apartado 1 del artículo 2. Con la intención en él referida, es castigado con pena de prisión hasta 5 años.

Punto 11 - Quien, por cualquier medio, viaje o trate de viajar a un territorio distinto de su Estado de residencia o nacionalidad con vistas a la adhesión a una organización terrorista o a la comisión de hechos previstos en el apartado 1 del artículo 2, la intención en él referida, es castigada con pena de prisión hasta 5 años.

Punto 12 - Quien organice, financie o facilite el viaje o intento de viaje previstos en los números anteriores, es castigado con pena de prisión de hasta 4 años.

Artículo 5 bis. Punto 1. Quien, por cualquier medio, directa o indirectamente, suministre, recopile o retenga fondos o bienes de cualquier tipo, así como productos o derechos susceptibles de ser transformados en fondos, con la intención de ser utilizados o sabiendo que pueden ser utilizados, total o en parte, en la planificación, la preparación o la práctica de los hechos previstos en el apartado 1 del artículo 2, bien con la intención mencionada en el mismo o con la intención contemplada en el apartado 1 del artículo 3, con una pena de prisión de 8 a 15 años.

Artículo 3. Adición a la Ley nº 52/2003, de 22 de agosto. Se añade a la Ley nº 52/2003, de 22 de agosto, modificada por las Leyes n° 59/2007, de 4 de septiembre, 25/2008, de 5 de junio, y 17 de noviembre, del 3 de mayo, el artículo 6 bis, con la siguiente redacción:

Artículo 6 bis. Comunicación de decisión final condenatoria. Los tribunales envían a la Unidad de Coordinación Antiterrorista, a la mayor brevedad y en formato electrónico, certificados de las decisiones finales condenatorias dictadas en procedimientos incoados por la comisión de crímenes de terrorismo, organizaciones terroristas, terrorismo internacional y financiación del terrorismo.

Artículo 4. Entrada en vigor: La presente Ley entrará en vigor el día siguiente al de su publicación. Aprobada el 30 de abril de 2015. La Presidenta de la Asamblea de la República, MARÍA DE LA ASUNCIÓN A. ESTEVES. Promulgada el 12 de junio de 2015. Firmado. El Presidente de la República, ANÍBAL CAVACO SILVA. Refrendo el 15 de junio de 2015.El Primer Ministro, PEDRO PASOS COELHO"[144].

Las actualizaciones en la leyes antiterroristas, siguen en todos los países la misma dirección (se podría hablar de una estandarización). De todas ellas, el país que realiza una modificación más extensa en su ley antiterrorista es España, que suma a su perspectiva de asociación terrorista la figura del "terrorista individual"

[144] MINISTERIO PÚBLICO, PORTUGAL. (2015). PGDL (Procuradoria-Geral distrital de Lisboa, Lei nº 60/2015 de 24 de Junio que modifica la ley antiterrorista Portuguesa.

no contemplada hasta el momento. En el caso portugués, su ley ha sufrido más modificaciones y ha ido actualizándose de forma más progresiva.

II.3.2.- Estrategia portuguesa en ciberseguridad

La Ciberseguridad como una prioridad nacional: El creciente número de incidentes y ataques maliciosos, que tienen como objetivo las infraestructuras de información del gobierno, instituciones públicas y privadas, empresas y ciudadanos, ha venido a demostrar la necesidad del país de levantar una Estructura de Ciberseguridad Nacional, capaz de garantizar una gestión eficaz de crisis, coordinar la respuesta operativa a los ataques cibernéticos, desarrollar sinergias nacionales y mejorar la cooperación internacional en este campo, lo que hace converger a los Estados en políticas y estrategias cooperativas de combate a todas las formas de ataque cibernético. (Naciones Unidas, OTAN, EU, OSCE).

"El estado tendrá que desarrollar una "Política para el dominio de la información", se crea una Estrategia de la Información Nacional (EIN) y dentro de la Estrategia de Seguridad y Defensa del Estado (ENSD), surge la Estrategia Nacional de Seguridad de la Información (ENSI)"[145] (Anexo VII).

La Ciberseguridad debe desarrollase en el marco de la ENSI[146] y tanto Portugal como en general en todos los países occidentales, la Ciberseguridad se revela indisociable de la Ciberdefensa del Estado, Esto significa que no será posible garantizar la Ciberseguridad sin el levantamiento de una capacidad de Ciberdefensa (ilustración 31).

Es en el año 2013 cuando Portugal comenzó a plantearse la creación de una Estrategia Nacional de Ciberseguridad definida y aprobada oficialmente.

[145] INSTITUTO DE DEFENSA NACIONAL, PORTUGAL. (Diciembre 2013). Cuaderno 12: Estrategia de Información y seguridad en el ciberespacio Investigación conjunta IDN-CESEDEN.

[146] Estrategia Nacional de Seguridad de la Información.

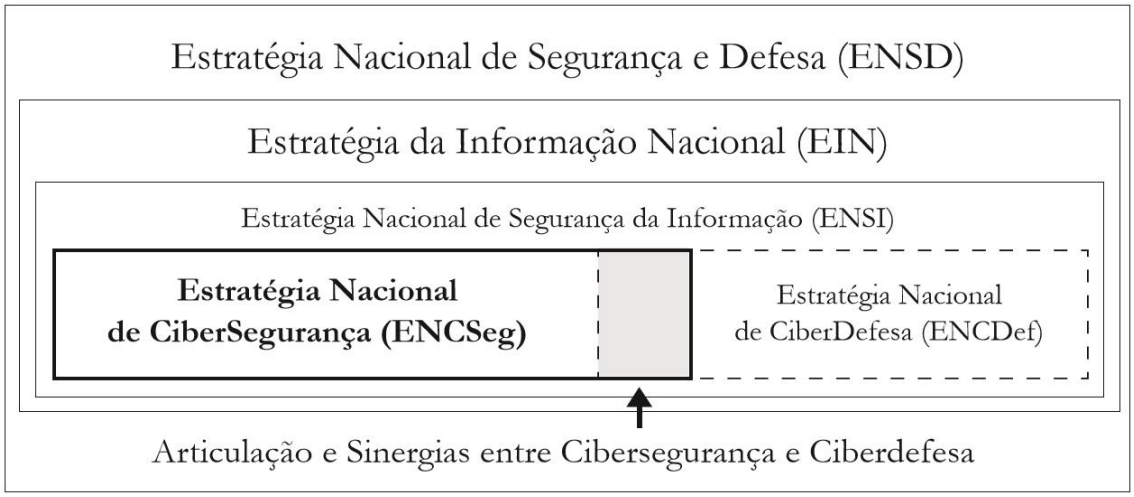


***Ilustración 31**: Marco de la Estrategia Nacional de Ciberseguridad*[147].

Empezaron realizando diversos trabajos de reflexión y grupos de trabajo oficialmente autorizados para trabajar en áreas comunes y para desarrollar una Estructura Nacional de Ciberseguridad[148] (La Comisión Instaladora del Centro Nacional de Ciberseguridad, la Oficina Nacional de Seguridad (GNS), (GECENI) Grupo de Estudio sobre las Contribuciones a una Estrategia Nacional de Información del Instituto de Defensa Nacional, intervenciones de la Autoridad Nacional de Seguridad (ANS) e intervenciones del Centro Gestión de la red informática). El 28 de Mayo del 2015 es cuando en el consejo de ministros (36/2015) se logra de conformidad con los artículos 199 (d)(f)(g) y 200(1ª) de la constitución Portuguesa firmar la aprobación y puesta en vigencia de la Estrategia nacional Portuguesa del ciberespacio (anexo VIII).

En la entrevista al Coronel NUNO CORREIA LEMOS PIRES, opina que "Las leyes y jueces de los países de la UE están preparados para actuar contra los delincuentes. Es un problema de mentalidad, no de legalidad. Los terroristas aprenden día a día y en la práctica buscan esquivar las barreras legales; depende en cada caso de los medios que tengan.Para el ciudadano es difícil conectar con las fuerzas de seguridad. Las amenazas más peligrosas son las armas nucleares o químicas; para acabar con ellas la mejor estrategia es la de ir a los países de

[147] INSTITUTO DE DEFENSA NACIONAL, PORTUGAL. (Diciembre 2013). Ob. Cit., p. 52, Figura 2 - Marco de la Estrategia Nacional de Ciberseguridad.

[148] Resolución del Consejo de Ministros nº 42/2012, Diario de la República, 1ª serie, nº 74, 13 de abril de 2012, fue nombrada una Comisión Instaladora del Centro Nacional de Ciberseguridad para desarrollar un marco estratégico para la futura estructura de ciberseguridad nacional.

origen y actuar allí, de esta forma los resultados han mejorado. La ciberseguridad en Portugal y la UE ha subido de nivel considerablemente. La PESCO (*Permanent structured cooperation*, cooperación estructurada permanente) firmada recientemente con la OTAN se traduce en un mayor instrumento de acción en defensa"[149].

El objetivo a alcanzar por la Estrategia Nacional de Ciberseguridad[150], es el de estimular una utilización libre, segura y eficiente del ciberespacio por parte de todos los ciudadanos, al tiempo que garantiza la protección y defensa de su infraestructura de información crítica en el plano de la seguridad de la información *(Information Assurance)* basándose en los principios generales de la soberanía estatal, las ideas generales contenidas en la Estrategia de ciberseguridad de la UE y en la estricta observancia del Convenio Europeo de Derechos Humanos, la Carta de los Derechos Fundamentales de la UE, la protección de los derechos fundamentales, libertad de expresión, datos personales y privacidad.

Esta visión se basa en cinco pilares: la subsidiariedad, complementariedad, cooperación, proporcionalidad y conciencia. Aunque sea el estado subsidiario de la defensa nacional, la responsabilidad de ésta es complementaria de todos los actores desde el individuo como usuario hasta los organismos de defensa y siempre con la idea de la cooperación entre los organismos de ciberseguridad tanto nacionales como internacionales para poder actuar de forma proporcional a los ataques: en definitiva crear una conciencia general de ciberseguridad.

Los **principales objetivos de la estrategia de ciberseguridad** son:

- Promover el uso consciente, libre, seguro y eficiente del ciberespacio.
- Proteger los derechos fundamentales, la libertad de expresión, los datos personales y la privacidad de los ciudadanos.
- Fortalecer y garantizar la seguridad del ciberespacio, de las infraestructuras

[149] Entrevista al Coronel NUNO CORREIA LEMOS PIRES por PONS GAMÓN. Academia Militar Portuguesa (2018), prácticas de movilidad internacional.

[150] GOBIERNO DE PORTUGAL. (2015).National Cyberspace Security Strategy. Recuperado de: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf

críticas y de los servicios nacionales vitales.

- Afirmar el ciberespacio como un lugar para el crecimiento económico y la innovación.

A continuación, veremos las líneas de acción de la estrategia de ciberseguridad portuguesa de 2015 (ilustración 32).

ESTRATEGIA DE CIBERSEGURIDAD PORTUGUESA 2015:
LINEAS DE ACCIÓN

Estructura de la seguridad del ciberespacio: La seguridad del ciberespacio requiere un liderazgo y un gobierno sólido y multidisciplinar, una coordinación operativa ágil, receptiva y efectiva; la capacidad de responder y proteger el interés nacional y sobre todo, el acceso a recursos, conocimientos y habilidades. Adoptando 6 medidas:

1) Establecer una coordinación político-estratégica para la seguridad y defensa del ciberespacio.
2) Consolidar la coordinación operativa y la función de autoridad nacional del Centro Nacional de Ciberseguridad (CNCS):
   a) Confirmar el derecho de CNCS a operar como autoridad nacional competente.
   b) El CNCS supervisará la coordinación entre las diversas partes responsables.
   c) La seguridad del ciberespacio presupone una comprensión de las amenazas y vulnerabilidades existentes.
   d) La CNCS, debe desarrollar e implementar medidas que garanticen las capacidades humanas y tecnológicas de las infraestructuras públicas y críticas
   e) Establecer condiciones para establecer un nivel de alerta nacional en materia de ciberseguridad.
   f) CNCS compilará una base de conocimientos que contendrá información sobre amenazas y vulnerabilidades conocidas, que se pondrá a disposición de los organismos públicos y los operadores de infraestructuras críticas
   g) La CNCS debe producir y presentar una imagen completa y actualizada de todos los incidentes, amenazas y vulnerabilidades al ciberespacio nacional.
3) :Desarrollar la capacidad para la defensa cibernética:
   a) Implementar la Guía de Políticas de Defensa Cibernética.
   b) Establecer y consolidar una estructura nacional de comando y control de la ciberdefensa con las fuerzas armadas.
   c) Implementar, desarrollar y consolidar capacidades de defensa cibernética que garanticen operaciones militares en el ciberespacio.
   d) Hacer de la ciberdefensa un área donde sea necesario promover sinergias y fomentar el doble uso de sus capacidades (en el ámbito militar).
4) :Mejorar la capacitación de seguridad en el ciberespacio:
   a) El rol de las (CSIRT) debe fortalecerse como plataforma de excelencia para compartir buenas prácticas e información sobre incidentes cibernéticos.
   b) Los diversos CSIRT deben usar una taxonomía común y mecanismos automáticos para compartir información operativa entre ellos y con las fuerzas y servicios de seguridad.
5) Establecer una oficina para gestionar las crisis del ciberespacio:
   a) La respuesta a incidentes cibernéticos de alto impacto requiere procedimientos

específicos y especiales.
   b) Los ejercicios de gestión de crisis nacionales en el ciberespacio deben organizar y desarrollar para permitir la evaluación del nivel de preparación.
6) Definir e implementar el gobierno del ciberespacio y los procesos de seguridad.

Abordando el cibercrimen: Los desafíos que plantea el delito cibernético significan que las leyes deben actualizarse constantemente para garantizar su máxima efectividad y las instituciones adaptarse a las nuevas tecnologías. Adoptando 2 medidas:
1) Revisar y actualizar la legislación.
2) Mejorar los poderes de la Policía Criminal Portuguesa (Policía Judicial).

Protección del ciberespacio y las infraestructuras: Las amenazas a las infraestructuras y los sistemas de información están dirigidas tanto a los organismos públicos como a los privados y a los ciudadanos. Adoptando 13 medidas:
1) Evaluar la madurez y la capacidad de los organismos públicos y privados que administran las infraestructuras críticas y los servicios de información vital.
2) Promover la adaptación y mejora continua de la seguridad de todos los sistemas de información.
3) Analizar el entorno de información para anticipar posibles ataques y tomar las medidas necesarias.
4) Desarrollar la capacidad de detectar ataques a los sistemas de información.
5) Promover en organismos públicos la implementación de medidas necesarias de respuesta para garantizar su continuidad después de un ataque.
6) Incluir medidas de seguridad en el ciberespacio en los planes nacionales de protección de infraestructuras críticas.
7) Incluir medidas para abordar las amenazas ciberespaciales a los planes de seguridad de los operadores de infraestructuras críticas nacionales y europeas
8) Promover el uso de normas de seguridad de la información para las infraestructuras de información y comunicaciones del cuerpo público.
9) Promover una política de seguridad de la información para los organismos públicos
10) Mejorar la capacidad de prevenir, detectar y responder a incidentes de seguridad en el ciberespacio.
11) Evaluar y desarrollar marcos regulatorios sectoriales.
12) Adaptar la legislación nacional para responder a los avances tecnológicos y las nuevas prácticas.
13) Garantizar y proteger las infraestructuras de información críticas a través de un Sistema Nacional de Protección de Infraestructura de Información (SPIIN).

Educación, Conciencia y Prevención: Promover una cultura de seguridad que proporcione recursos humanos cualificados. Adoptando 8 medidas:
1) Promover campañas de información y alertas para todos los ciudadanos y empresas.
2) Sensibilizar a los operadores públicos y privados sobre la naturaleza crítica de la seguridad informática.
3) Promover una cultura de seguridad en el ciberespacio a través de campañas e iniciativas que se coordinen y desarrollen con un enfoque común y positivo.
4) Mejorar la capacitación de seguridad en el ciberespacio.
5) Promover el uso seguro de las TIC y el ciberespacio.
6) Promover la capacitación especializada en seguridad del ciberespacio.
7) Promover la capacitación especializada de los responsables de la toma de decisiones
8) Establecer programas especiales para pequeñas y medianas empresas (PYME).

Investigación y desarrollo: Desarrollar y apoyar iniciativas tecnológicas conjuntas de empresas, ejército y universidades. Adoptando 5 medidas: 1) Promover la investigación científica y el desarrollo en seguridad del ciberespacio. 2) Estimular y mejorar las capacidades científicas, industriales y humanas de la nación independiente. 3) Apoyar la participación nacional en proyectos internacionales. 4) Maximizar las sinergias resultantes de foros. 5) 5) Explotar la experiencia adquirida.

Cooperación: La ciberdefensa exige la cooperación cerrada entre socios y aliados nacionales e internacionales. Adoptando 4 medidas: 1) Desarrollar iniciativas de cooperación: en seguridad de los sistemas de información, ciberdelincuencia, defensa cibernética y terrorismo cibernético, ciberespionaje y ciberdelincuencia. 2) Cooperación-colaboración multilateral: EU y OTAN principalmente 3) Participar y cooperar con los foros de CSIRT. 4) Participar en ejercicios de seguridad en el ciberespacio, especialmente en el contexto de la UE y la OTAN.

***Ilustración 32**: Líneas de acción estrategia de la seguridad Portuguesa[151].*

Un punto importante en el cual la estrategia de ciberseguridad hace hincapié al finalizar, es su revisión constante y periódica. Esta debe ser revisada en periodos inferiores a tres años y cada año se deben verificar los objetivos estratégicos, las líneas de acción y su adaptación a las circunstancias cambiantes.

II.3.3.- Iniciativas comunes en ciberseguridad entre España y Portugal

Siguiendo las iniciativas actuales y futuras, siguiendo la estrategia de cooperación y estandarización, la doctrina en ciberseguridad de ambos países es cada vez más convergente, buscando una estrategia común.

Portugal y España se desenvuelven en las principales organizaciones internacionales (OTAN, UE, ONU / UIT y la OCDE), que a su vez repercuten en todos sus ámbitos social, operativo, estratégico y económico, identificando las áreas estratégicas comunes de cooperación internacional en el Ciberespacio. De esta formam se estructuran los objetivos estratégicos a alcanzar y los elementos

[151] Elaboración propia. Trabajo Academia militar Portuguesa, Prácticas de movilidad, realizadas en el marco del programa internacional. tabla-esquema: Líneas de acción estrategia de la Ciberseguridad portuguesa 2015.

asociados en el ámbito de la ciberseguridad y la ciberdefensa (ilustración 47, del anexo III).

Para Portugal y España (ver Anexo III) la base fundamental es la cooperacion civil y militar dentro del ámbito de la OTAN (militar) y la UE (inmigración).

En la entrevista realizada a la profesora CASIMIRO (2018), indica que "La lucha contra el terrorismo requiere una respuesta coordinada internacionalmente, tanto en el mundo analógico como en el mundo digital. En el contexto particular de la Unión Europea, se necesita un marco jurídico más amplio para armonizar el análisis forense digital, regular las operaciones de red ofensivas y defensivas, aclarar el procesamiento de los datos generados por el uso de servicios de comunicaciones electrónicas e implementar procedimientos idénticos para bloquear, eliminar o restringir el acceso a contenidos en línea que consisten en reclutamiento y entrenamiento para el terrorismo y provocación pública para cometer delitos de terrorismo".

"El Reglamento general de protección de datos y algunas de las decisiones del Tribunal de Justicia de las Comunidades Europeas, como la declaración de nulidad de la Directiva de conservación de datos o el reconocimiento del derecho a conectarse a Internet, han representado un paso importante en la defensa de la privacidad y la libertad de información en el mundo digital y, en última instancia, al hacer hincapié en la importancia de los derechos fundamentales en el ordenamiento jurídico de la Unión Europea. Sin embargo, esto es solo la mitad de la ecuación. Es igualmente importante establecer claras restricciones a los derechos fundamentales en el mundo digital para fines específicos del orden público. En lo que respecta al terrorismo, ésto aún está por hacerse"[152].

Para finalizar tratamiento sobre Portugal y a modo también de síntesis o conclusión, ya que en nuestraopinión abarca tanto el ámbito legal como el ámbito operativo, enriqueciendo notablemente este apartado, adjuntamos, en el anexo VI, las preguntas entrevistasrealizadas en esta investigación, en las cuales abordamos interrogantes sobre aspectos legales, posibles obstáculos o vacios y

[152] Entrevista a la profesora CASIMIRO por PONS GAMÓN, V. (2018). Encuestas Academia Militar Portuguesa (2018), Prácticas de movilidad internacional.

preparación de los Jueces y Fiscales, aspectos generales como posibles amenazas terroristas y el funcionamiento del sistema de denuncia ciudadana en caso terrorista y también, por último, aspectos operativos como la preparación de Portugal en ciberdefensa y su cooperación internacional.

En este sentido, SILVA VIEIRA[153], señala[154]: "Portugal tiene actualmente los instrumentos jurídicos necesarios para sus fuerzas y servicios de seguridad para reaccionar eficazmente contra cualquier acción terrorista. La Estrategia Nacional de Lucha contra el Terrorismo (Resolución del Consejo de Ministros nº 7/2015, de 19 de febrero) enmarca una ola de modernización y actualización del contexto jurídico y normativo en lo que concierne a la lucha contra el terrorismo.

Al alinearse con las medidas de lucha contra el terrorismo recomendadas tanto a nivel de la Unión Europea como de la OTAN y de las Naciones Unidas, la Estrategia tuvo como primera consecuencia práctica la institucionalización de la UCAT (Unidad de Coordinación Antiterrorismo), que es el órgano de coordinación y reparto de información, en el marco de la amenaza y la lucha contra el terrorismo, entre las entidades que la integran (las Fuerzas y Servicios de Seguridad). La modificación a la Ley de Seguridad Interna (Ley nº 53/2008, de 29 de agosto) operada por la Ley nº 59/2015, de 24 de junio, institucionaliza la organización y el funcionamiento de la UCAT.

Además de estas alteraciones se adoptaron medidas de criminalización de la apología pública y los desplazamientos hacia la práctica del terrorismo (Ley 60/2015, de 24 de junio que alteró la Ley de Combate al Terrorismo, Ley 52/2003, 22 agosto), de lucha contra el blanqueamiento de fondos (Ley 58/2015, 23 de junio), modificada la Ley Organización de la Investigación Criminal (Ley 49/2008, 27 de agosto), modificada el Código Penal, actualizando la definición de terrorismo (Ley 58/2015, 23 de junio) para abarcar crímenes terroristas (Ley 57/2015, 23 de junio) y medidas de combate al crimen organizado y económico-financiero relacionado con el terrorismo (Ley 55/2015, de 23 de junio). Más recientemente, se aprobó el procedimiento especial de acceso a datos de telecomunicaciones e

[153] Dr. MANUEL SILVA VIEIRA, Secretaría Permanente, Sistema de seguridad interior (SSI), Gobierno de Portugal.

[154] Entrevista al Dr. MANUEL SILVA VIEIRA por PONS GAMÓN. Academia militar Portuguesa (2018), prácticas de movilidad internacional.

Internet por los oficiales de información del Servicio de Información de Seguridad y del Servicio de Información Estratégica de Defensa (Ley Orgánica nº 4/2017, de 25 de agosto) para efectos de la producción de información necesaria para la prevención de actos de espionaje y terrorismo.

Los magistrados portugueses (jueces y fiscales) están preparados para actuar con eficacia y rapidez en situaciones terroristas u organizaciones terroristas. En realidad, algunas de las modificaciones legislativas en materia judicial se produjeron tras una oleada de atentados terroristas (con inspiración ideológica en la izquierda radical) que tuvo lugar en la década de los ochenta del siglo XX. La coordinación de la dirección de los crímenes de organización terrorista y terrorismo es de la exclusiva competencia del Departamento Central de Investigación y Acción Penal, órgano de coordinación de la Procuraduría General de la República. De la misma manera, la competencia para la instrucción de crímenes de organización terrorista y terrorismo está atribuida a un tribunal central de instrucción. Esta centralización de la investigación y de la instrucción, de procesos que involucran actos terroristas denota bien la capacidad de especialización de los magistrados que integran dicho órgano.

La amenaza terrorista de matriz islamista es la más probable y peligrosa, tanto a nivel internacional como a nivel de la amenaza a la seguridad interna de Portugal. De entre los agentes de esa amenaza, no puede dejar de ser destacado el grupo conocido como Estado Islámico, que a pesar de haber sido derrocado en su territorio de implantación, puede seguir inspirando acciones terroristas, sobre todo en suelo europeo.

El modelo de policía nacional, que se basa en dos fuerzas de seguridad (GNR y PSP)[155], ambas de proximidad, es idóneo para detectar e identificar precozmente potenciales amenazas terroristas. La recogida, tratamiento y análisis de datos e información y su puesta a disposición recíproca entre entidades responsables en este ámbito permite anticipar el conocimiento y la evaluación de ofensivas en preparación, siempre en cooperación con entidades extranjeras.

[155] Guardia Nacional Republicana y Policía de seguridad Pública de Portugal.

El ciudadano puede recurrir a los mecanismos de emergencia (central 112) o a cualquier autoridad policial que tiene el deber y la capacidad de reaccionar en tiempo oportuno a cualquier amenaza terrorista.

La defensa cibernética se configura como una capacidad de las fuerzas armadas portuguesas y hay un centro de defensa cibernética, como parte de la Mayor de las Fuerzas Armadas. A este Centro, que depende de la Dirección de Comunicaciones y Sistemas de Información del EMGFA[156], corresponde asegurar y participar en la representación nacional en los organismos internacionales de Defensa, en el ámbito de la guerra electrónica y Ciberdefensa. El Centro Nacional de Ciberseguridad, que funciona desde 2014 (Decreto-Ley nº 69/2014, de 9 de mayo) actúa como coordinador operativo y autoridad nacional especialista en materia de ciberseguridad ante las entidades del Estado, operadores de servicios esenciales y prestadores de servicios digitales, garantizando que el ciberespacio se utilice como espacio de libertad, seguridad y justicia, para la protección de los sectores sociedad que materializan la soberanía nacional y el Estado de Derecho Democrático. Este Centro asegura la planificación de la utilización no militar del ciberespacio en situación de crisis o de conflicto armado en el marco de la planificación civil de emergencia y actúa en articulación y estrecha cooperación con las estructuras nacionales responsables del ciberespionaje, el ciberdefensa y el ciberdelincuencia y el ciberterrorismo, y con la Policía Judicial, comunicando los hechos de que tenga conocimiento relativo a la preparación y ejecución de crímenes.

Es importante subrayar, a este propósito, que la actuación del Centro Nacional de Ciberseguridad está perfectamente alineada con la Estrategia Nacional de Seguridad del Ciberespacio (Resolución del Consejo de Ministros nº 36/2015, de 28 de mayo), documento que está actualmente en fase de revisión. Esta Estrategia preconiza la cooperación (Eje 6) en áreas vinculadas a la seguridad de los sistemas de información, ciberdelincuencia, ciberdefensa y ciberterrorismo, ciberespionaje, ciberdiplomacia, para potenciar el conocimiento necesario para la protección de los sistemas de información nacionales. Esta

[156] Estado Mayor General de las Fuerzas Armadas de Portugal.

cooperación se produce en el marco de la Unión Europea (ENISA, por ejemplo), de la OTAN y otras entidades.

El coordinador del Centro Nacional de Ciberseguridad integra, desde 2015, el Consejo Superior de Seguridad Interna, que es el órgano interministerial de audición y consulta en materia de seguridad interna. Desde 2017 (Resolución del Consejo de Ministros nº 115/2017, de 13 de julio) el Secretario General del Sistema de Seguridad Interna integra el grupo de proyecto denominado Consejo Superior de Seguridad del Ciberespacio, que tiene por misión asegurar la coordinación político estratégica para la seguridad del ciberespacio y el control de la aplicación de la Estrategia Nacional de Seguridad del Ciberespacio"[157].

II.4.- ENTRAMADO EUROPEO EN CIBERSEGURIDAD

a) Introducción

En todo el contexto de la UE sus ciudadanos y sus economías cada vez necesitan más de las tecnologías digitales. La ciberseguridad es tan importante que de ella depende nuestra seguridad y por tanto nuestra prosperidad. Estas amenazas son un obstáculo tanto económico como social que intentan destruir nuestro estado de libertad, democracia y por supuesto nuestros valores.

Debemos reaccionar y tener en cuenta que nuestro futuro depende del control de esta ciberamenazas. Todo nuestro entramado tanto civil como militar depende de ello porque a su vez estos dependen de sistemas digitales.

Nuestra seguridad futura depende de la transformación de nuestra capacidad para proteger a la UE contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros.

En este tipo de amenaza existe una gran confusión de fronteras naturales y líneas de delitos tradicionales. No siempre estos ataques son realizados por

[157] Entrevista al Dr. MANUEL SILVA VIEIRA por PONS GAMÓN. Academia militar Portuguesa (2018), prácticas de movilidad internacional.

civiles (*ransomware*). Muchas veces se trata de determinados estados que no siguen las reglas de convivencia mundiales.

Las posibilidades de rastrear a los ciberdelincuentes están muy limitadas, ya que con medios escasos pueden conseguir resultados desastrosos sin ningún tipo de intervención militar.

El mundo cibernético se mueve tan rápido que para poder conseguir resultados es muy importante la cooperación internacional en todos sus ámbitos. Un simple fallo en los dispositivos que controlan nuestras infraestructuras eléctricas, finanzas, hospitales etc., puede ser en su base devastador.

Un enfoque establecido en trabajar hacia una comunicación conjunta hará que la UE esté mejor situada para hacer frente a estas amenazas. Desarrollaría una mayor capacidad de recuperación y autonomía estratégica, mejorando las capacidades en términos de tecnología y habilidades, además de ayudar a construir un mercado único fuerte.

La UE necesita de las estructuras adecuadas para disfrutar de una ciberseguridad robusta y efectiva cuando sea necesaria, que sea participativa total, intensificando la lucha para detectar, rastrear y mantener a raya a los ciberdelincuentes para que de esta forma se rechacen sistemáticamente estos ataques.

Estas **estrategias** están basadas en:

- Enfoques del Mercado Único Digital.
- La Estrategia Global.
- La Agenda Europea de Seguridad.
- El Marco Conjunto para contrarrestar las amenazas híbridas.

La UE ya está trabajando desde el 2013, con la establecida Estrategia de Ciberseguridad, basada en un ecosistema cibernético confiable, seguro y abierto. Pero el hábitat de amenazas evoluciona y se profundiza contínuamente y requiere más acción para resistir y disuadir ataques en el futuro.

Según esta estrategia, los Estados miembros siguen siendo responsables de su seguridad nacional.La escala y la naturaleza transfronteriza de la amenaza constituyen un argumento poderoso para la acción de la UE que ofrece incentivos y apoyo a los Estados miembros para desarrollar y mantener más y mejores capacidades nacionales de ciberseguridad, al mismo tiempo que capacidad a nivel de la UE. Esto supone un ente concreto para ayudar a detectar e investigar cualquier forma de incidentes cibernéticos contra la UE y sus Estados miembros y para responder adecuadamente, incluso mediante el enjuiciamiento de delincuentes.

"La Asociación Público-Privada en Ciberseguridad"[158]creada en 2016 fue un primer paso importante, que provocó hasta 1.800 millones de euros de inversión para 2020. Sin embargo, la escala de la inversión en curso en otras partes del mundo[159]sugiere que la UE necesita hacer más en términos de inversión, para superar la fragmentación de las capacidades repartidas en toda la UE.La Unión Europea ha agregado valor para proporcionar, dada la sofisticación de la tecnología de ciberseguridad, la inversión a gran escala requerida y la necesidad de soluciones que funcionen en toda la UE. Sobre la base del trabajo de los Estados miembros y la Asociación Público-Privada, un paso más sería reforzar la capacidad de ciberseguridad de la UE a través de una red de centros[160]de competencia en ciberseguridad con un Centro Europeo de Investigación y Competencia de Ciberseguridad en su corazón. Esta red y su Centro estimularían el desarrollo y el despliegue de tecnología en ciberseguridad y complementarían los esfuerzos de desarrollo de capacidades en esta área a nivel nacional y de la UE. La Comisión lanzará una evaluación de impacto para examinar las opciones disponibles, incluida la posibilidad de establecer una empresa común, con vistas a establecer esta estructura en 2018. Como primer paso y para informar sobre las ideas futuras, la Comisión propondrá que se inicie un programa piloto. Se lanza la fase bajo Horizonte 2020 para ayudar a reunir centros nacionales en una red para

[158] Asociación creada por la Comisión Europea el 05-07-2016, como iniciativa destinada a equipar mejor a Europa contra los ciberataques y reforzar su sector de ciberseguridad.

[159] THE WHITE HOUSE. OFFICE OF THE PRESS SECRETARY. (2016). *The US will invest 19 billion dollars in cybersecurity in 2017 alone, a 35 % increase compared to 2016. 'Fact Sheet: Cybersecurity National Action Plan', 9 February 2016.*

[160] La red incluiría centros de ciberseguridad existentes y futuros establecidos en los Estados miembros, cuyos miembros serían normalmente organizaciones públicas de investigación y laboratorios.

crear un nuevo impulso en competencia de ciberseguridad y desarrollo de tecnología. Planea proponer una inyección de financiación a corto plazo de 50 millones de euros para este fin. Esta actividad complementará la implementación en curso de la Asociación Público-Privada en Ciberseguridad" *(traducción propia)*[161].

b) Defensa de la UE ante los ataques cibernéticos

Son necesarias estructuras mucho más sólidas y eficaces para promover la ciberseguridad y para responder a los ciberataques en los Estados miembros, pero también en las propias instituciones y organismos de la UE. Requiere un enfoque amplio y de políticas cruzadas, construir una resistencia cibernética con una estratégica autónoma, en un mercado único sólido de avances en capacidad tecnológica y un número muy alto de expertos cualificados.

La ciberseguridad es un desafío social común donde deben participar gobierno, economía y sociedad.

La Agencia de Seguridad de la Red y de la Información de la Unión Europea (ENISA) tiene un papel clave en el fortalecimiento de la resistencia y respuesta cibernética de la UE. Limitada por su mandato actual, la Comisión ha presentado una propuesta de reforma con un mandato permanente para la agencia. Esta brindará apoyo a los Estados miembros, instituciones de la UE y a las empresas en áreas clave; tendrá papel clave de asesoría en el desarrollo y la implementación de políticas, ayuda para establecer centros de intercambio y análisis de información en sectores críticos. ENISA aumentará la presión y prepara ejercicios paneuropeos de ciberseguridad, certificación de ciberseguridad e intensifica la cooperación operativa y la gestión de crisis en toda la UE.

La agencia también sirve como punto de información y conocimiento en la comunidad de seguridad cibernética. Esto requiere la participación de todos los

[161] Vid.EUROPEAN COMMISSION. (13 de septiembre de 2017). High representative of the unión for foreign affairs and security policy. Joint communication to the European parliament and the council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 8 and 9, Brussels.

actores relevantes (órganos y organismos de la UE, así como Estados miembros) a nivel técnico, operacional y estratégico.

Colaboran también organismos como la red de equipos informáticos de respuesta a incidentes de seguridad, CERT-EU, Europol y el Centro de Inteligencia y Situación de la UE (INTCEN), que contribuyen a la conciencia situacional a nivel de la UE.

Ir hacia un mercado único de ciberseguridad, tiene la consecuencia que la Comisión presente una propuesta para establecer un marco de certificación de la seguridad cibernética de la UE. Este marco establecerá el procedimiento para la creación de sistemas de certificación de ciberseguridad en toda la UE. Esto es beneficioso para las empresas, pues evita la necesidad de pasar por varios procesos de certificación por fronteras, y limita los costos administrativos y financieros.

Este certificado de conformidad informa y tranquiliza a los compradores y usuarios de servicios que compran y usan.

Los esquemas del Marco serían voluntarios y no crearían ninguna obligación regulatoria inmediata sobre los clientes o proveedores de servicios. Los esquemas no estarían en contradicción con los requisitos legales aplicables, como la legislación de la UE en materia de protección de datos.

Seguidamente observamos los puntos fuertes:

- El uso de herramientas no debe conducir a nuevas fuentes de riesgo o nuevas vulnerabilidades.
- Utilizar métodos que han sido sometidos a pruebas de seguridad adecuadas y actualizar su software en caso de vulnerabilidades o amenazas recientemente descubiertas.
- "Necesitamos proteger mejor a los europeos en la era digital. En los últimos tres años, hemos progresado para mantener a los europeos seguros en línea. Las nuevas reglas, presentadas por la Comisión, protegerán nuestra propiedad intelectual, nuestra diversidad cultural y nuestros datos personales. Hoy, la Comisión propone nuevas herramientas" *(traducción*

propia)[162].

c) Resumen de conceptos clave en la línea de ciberseguridad europea

EN SEGURIDAD:

- Se percibe de forma global el ciberdelito como una amenaza a la seguridad.
- Importancia del crecimiento exponencial de la ciberdelincuencia.
- Activación de la acción de las autoridades nacionales encargadas de hacer cumplir la ley en la lucha contra el cibercrimen.

EN SEGURIDAD CIBERNÉTICA

1. Uso de Internet.

a) Frecuencia de acceso a Internet.

b) Medios de acceso a Internet.

c) Actividades en línea.

2. Preocupaciones sobre las transacciones de Internet.

a) Preocupaciones.

b) Impacto en el comportamiento.

3. Conciencia y experiencia de ciberdelitos.

- Nivel de conocimiento.

[162] JUNCKER, J-C. (13 September 2017). *European Commission. State of the Union Address. Cibersecuriy tackling non-cash payment frau, p. 1, Brussels*.

- Actitudes hacia la seguridad cibernética.
- Preocupaciones y experiencia de ciberdelitos específicos.
- Lucha contra el cibercrimen.
- Las instituciones percibidas como responsables de proporcionar asistencia a los ciudadanos para los diferentes tipos de ciberdelitos, acciones y experiencia en ciberdelitos específicos.

Tipos de ciberdelitos:

1. Robo de identidad.
2. E-mails o llamadas telefónicas de estafa.
3. Fraude en línea.
4. Material ofensivo y pornografía infantil.
5. Material que promueve el odio racial o el extremismo religioso.
6. Acceso a servicios en línea.
7. Piratería de cuentas de correo electrónico.
8. Fraude bancario en línea.
9. Extorsión cibernética.
10. Software malicioso.

"El delito cibernético es un problema sin fronteras, que consiste en actos delictivos que se cometen en línea mediante el uso de redes de comunicaciones electrónicas y sistemas de información. Los principales tipos de crímenes que se cometen de esta manera incluyen ataques a sistemas de información que pueden obstaculizar o deshabilitar su funcionamiento, formas de fraude y falsificación en línea como robo de identidad y código malicioso, y la difusión de contenido ilegal en línea como pornografía infantil. Se estima que el cibercrimen causa la pérdida de miles de millones de euros por año y está ejerciendo una presión cada vez mayor sobre la capacidad de respuesta de las fuerzas del orden. Con el creciente uso de Internet, la proliferación de diferentes tipos de dispositivos habilitados para Internet y una creciente cantidad de datos personales que se transmiten en línea, el problema del cibercrimen sólo empeorará a menos que las autoridades adopten

medidas concertadas para erradicarlo. En respuesta a este creciente problema, la Comisión Europea ha diseñado una política coordinada en estrecha cooperación con los Estados miembros de la Unión Europea (UE)[163].

Las acciones legislativas de la UE que contribuyen a la lucha contra el cibercrimen abordan cuestiones como los ataques contra los sistemas de información, el material ofensivo en línea y la pornografía infantil, la privacidad en línea y el fraude y la falsificación en línea. El objetivo de esta encuesta es comprender la conciencia, las experiencias y las percepciones de los ciudadanos de la UE sobre cuestiones de ciberseguridad" *(traducción propia)*[164].

d) Agencia europea garante del marco de certificación

Con el afán hacer mas efectivo e incrementar la respuesta a los ciberataques, para aumentar la confianza en el mercado único digital, la Comisión Europea propuso la creación de una Agencia de Ciberseguridad propia, basada en la Agencia Europea para la Seguridad de las Redes y la Información (ENISA) para mejorar la coordinación y cooperación entre los Estados miembros e instituciones, agencias y organismos internos.

Se establece un marco de certificación de ciberseguridad en la UE para garantizar el uso de dispositivos ("Internet de las cosas"), infraestructuras críticas actuales, redes de energía y transporte, y nuevos dispositivos de consumo.

Una Agencia de Seguridad Cibernética de la UE con un mandato fuerte, permanente que goce de los recursos adecuados.

"ENISA mejorará la preparación de la UE para reaccionar, organizando ejercicios anuales de ciberseguridad paneuropea y contribuyendo a un mejor intercambio de información entre los Estados miembros a través de la red de

[163] Vid. Más información sobre la lucha contra la cibercriminalidad en la UE en: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[164] Encuesta solicitada por la Comisión Europea, Dirección General de Migración y Asuntos de Interior y coordinada por la Dirección General de Comunicación (Junio de 2017. Publicada en septiembre de 2017). EUROPEAN COMMISSION. (Junio de 2017. Publicada en septiembre de 2017). Dirección General de Migración y Asuntos de Interior y coordinada por la Dirección General de Comunicación *Eurobarómetro especial 464ª*, Las actitudes de los europeos hacia la ciberseguridad, Bruselas..

Equipos de respuesta a incidentes de seguridad informática (CSIRT). Ayudará a los Estados miembros a aplicar la Directiva sobre seguridad de las redes y sistemas de información (NIS) que aclara las obligaciones de información de las autoridades nacionales en caso de incidentes graves.

ENISA tiene los siguientes recursos:

- Personal: Ahora, 84 personas. En el futuro, 125 personas.
- Presupuesto, ahora 11 millones de €. En el futuro 23 millones de €. Aumento gradual: comenzando con 5 millones en el primer año y completamente logrado 4 años después de la entrada en vigencia.
- Desarrollo e implementación de políticas: fortalecer el apoyo a la Comisión y los Estados Miembros en el desarrollo, implementación y revisión de la política general de ciberseguridad y en los sectores estratégicos clave identificados por la directiva NIS, p.ej. energía, transporte y finanzas.
- Conocimiento e información: para proporcionar análisis y consejos y concienciar, para convertirse en la ventanilla única *(InfoHub)* de la información de ciberseguridad de las instituciones y organismos de la UE.
- Creación de capacidad: reforzar el apoyo a los Estados Miembros con el fin de mejorar las capacidades y los conocimientos especializados, por ejemplo, en la prevención y respuesta a incidentes.

Las tareas relacionadas con el mercado dentro del Marco de Certificación de Ciberseguridad preparan los esquemas de certificación europeos de ciberseguridad, con la asistencia de expertos y la estrecha cooperación de las autoridades nacionales de certificación. Los esquemas serían adoptados por la Comisión. ENISA también apoyará el desarrollo de políticas en la estandarización de tecnologías de la información y la comunicación (TIC) (*traducción propia)*[165].

[165] EUROPEAN COMMISSION. (2017). State of the Union. Cybersecurity EU Agency and Certification Framework, page 1, Brussels.

e) Preguntas clave en la línea de ciberseguridad europea

- ¿Por qué la UE necesita tomar medidas sobre ciberseguridad?

Desde 2013, el ambiente tecnológico y de seguridad en la Unión Europea se mueve a un ritmo vertiginoso. Este es ahora parte integral de nuestro día a día y la columna central de nuestra economía, con decenas de miles de millones de dispositivos que se espera estén conectados a Internet para 2020. De la misma forma el número y la diversidad de las amenazas cibernéticas aumentan continuamente.

Para que el ciberespacio permanezca abierto y libre, las mismas normas, principios y valores que la UE defiende tienen que aplicarse también en en este nuevo espacio, así los derechos fundamentales, la democracia y el estado de derecho tienen que estar protegidos en el ciberespacio. Nuestra libertad y prosperidad dependen cada vez más de un Internet robusto e innovador. Pero todos estos derechos y libertades en la red también requieren seguridad. El ciberespacio debe estar protegido de incidentes, actividades maliciosas y uso indebido; y los gobiernos tienen una función importante para garantizar un ciberespacio libre y seguro. Es por ello que la Comisión Europea publicó un comunicado conjunto del Parlamento, el Consejo, el Comité Económico y social y el Comité de las Regiones sobre la "Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto y seguro" (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*)[166].

La UE necesita ser más resistente y efectiva a los ciberataques, y debe desarrollar más en este sentido el derecho penal, para proteger mejor a ciudadanos, empresas e instituciones públicas de Europa.

"El 13 de septiembre, en su discurso anual sobre el Estado de la Unión, el presidente JEAN-CLAUDE JUNCKER declaró: "En los últimos tres años, hemos progresado para mantener a los europeos seguros en línea. Pero Europa todavía no está bien equipada cuando se trata de ciberataques. Por eso, hoy, la Comisión

[166] Vid. EUROPEAN COMMISSION. (7 de febrero de 2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Recuperado de: https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

propone nuevas herramientas, incluida una Agencia Europea de Ciberseguridad, para ayudarnos a defendernos de tales ataques".

Los europeos depositan gran confianza en las tecnologías digitales. Abren nuevas oportunidades para que los ciudadanos se conecten, facilitan la difusión de información y forman la columna vertebral de la economía europea. Sin embargo, también han ocasionado nuevos riesgos a medida que actores no estatales y estatales intentan cada vez más robar datos, cometer fraude o incluso desestabilizar a los gobiernos. El año pasado, hubo más de 4.000 ataques de ransomware por día y el 80% de las empresas europeas experimentaron al menos un incidente de seguridad cibernética. El impacto económico del delito cibernético se ha quintuplicado solo en los últimos cuatro años. Para equipar a Europa con las herramientas adecuadas para hacer frente a los ciberataques, la Comisión Europea y el Alto Representante proponen un amplio conjunto de medidas para construir una ciberseguridad sólida en la UE. Esto incluye una propuesta de una Agencia de Seguridad Cibernética de la UE para ayudar a los Estados miembros a abordar los ciberataques, así como un nuevo esquema de certificación europeo que garantizará que los productos y servicios en el mundo digital sean seguros de usar.

FEDERICA MOGHERINI, Alta Representante/Vicepresidenta, declaró: "La UE perseguirá una política para promover un ciberespacio abierto, libre y seguro, así como apoyar los esfuerzos para desarrollar normas de comportamiento estatal responsable, y aplicar el derecho internacional y las medidas de fomento de la confianza en ciberseguridad."

ANDRUS ANSIP, Vicepresidente del Mercado Único Digital, indicó que:" Ningún país puede enfrentar los desafíos de ciberseguridad solos. Nuestras iniciativas fortalecen la cooperación para que los países de la UE puedan enfrentar estos desafíos juntos. También proponemos nuevas medidas para impulsar la inversión en innovación y promover la ciberhigiene".

JULIAN KING, Comisionado para la Unión de Seguridad, añadió que:" Necesitamos trabajar juntos para desarrollar nuestra capacidad de recuperación, impulsar la innovación tecnológica, impulsar la disuasión, reforzar la trazabilidad y la responsabilidad y aprovechar la cooperación internacional para promover

nuestra seguridad cibernética colectiva".

MARIYA GABRIEL, comisionada para la Economía y Sociedad Digitales, concluyó que:" Debemos construir sobre la base de la confianza de nuestros ciudadanos y empresas en el mundo digital, especialmente en un momento en que los ataques cibernéticos a gran escala son cada vez más comunes. Quiero que los altos estándares de seguridad cibernética se conviertan en la nueva ventaja competitiva de nuestras empresas". "Con recientes ataques *ransomware*, un aumento dramático en la actividad ciberdelincuente, el uso creciente de herramientas cibernéticas por parte de actores estatales para cumplir sus objetivos geopolíticos y la diversificación de incidentes de ciberseguridad, la UE necesita construir una mayor resistencia a los ciberataques y crear una respuesta eficaz de ciberdelincuencia y penal de la UE para proteger mejor a los ciudadanos, las empresas y las instituciones públicas de Europa. De esto se trata el paquete de seguridad" *(traducción propia)*[167].

- ¿Por qué la Comisión propone una Agencia de Seguridad Cibernética sólida de la UE?

La Comisión ha decidido adelantar la evaluación y revisión del mandato de la Agencia con sede en Grecia que expira en 2020, debido a los grandes cambios que se han producido en el mundo de la ciberseguridad desde la incorporación del Reglamento ENISA. Este proporcionaba experiencia y asesoramiento. La idea es que ahora debe actuar también de forma operativa.

La Directiva sobre la seguridad de las redes y los sistemas de información (NIS), tiene como objetivo "un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales"[168], ha creado formalmente una red de equipos de respuesta a

[167] Vid.EUROPEAN COMMISSION. (19 de septiembre de 2017a). *Press release: The Commission scales up response to cyberattacks, pag. 1. Brussels*.

[168] EUROPEAN UNION. (19 de julio de 2016). 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 en la Unión (Directiva sobre ciberseguridad NIS). Recuperado de: http://noticias.juridicas.com/base_datos/Admin/579387-directiva-2016-1148-ue-de-6-jul-medidas-destinadas-a-garantizar-un-elevado.html

incidentes de seguridad informática (CSIRT) de los Estados miembros y ENISA proporciona la secretaría para esta red.

Europa quiere transformar a ENISA en la Agencia de Seguridad Cibernética más sólida de la UE con un mandato permanente, con más recursos operativos y a largo plazo.

El objetivo principal de la Agencia es complementar a los Estados miembros a implantar la Directiva NIS.

En materia de certificación ENISA y las autoridades de certificación de los Estados miembros deben cooperar, pero el mandato, objetivos y tareas de la nueva Agencia estarán sujetos a revisiones periódicas.

- ¿Cuáles son las principales ciberamenazas para la UE?

El informe anual "ENISA *Threat Landscape Report* 2017: 15 *Top Cyber-Threats and Trends*", de enero de 2018, indica las principales ciberamenazas de 2017[169], así las 15 amenazas identificadas son: 1. Malware; 2. Web based attacks; 3. Web application attacks; 4. Phishing; 5. Spam; 6. Denial of service; 7. Ransomware; 8. Botnets; 9. Insider threat; 10. Physical manipulation/damage/ theft/loss; 11. Data breaches; 12. Identity theft; 13. Information leakage; 14. Exploit kits; 15. Cyber espionaje. En el citado informe se observa un incremento del Phising, spam, ransomware, exfiltración de información y robo de identidad, en relación al informe emitido el año anterior. También comenta que la complejidad de los ataques y su sofisticación continúan aumentanto y existe en las organizaciones una gran preocupación por la falta de capacitación y preparación para hacer frente a estas amenazas.

- ¿Por qué propone la Comisión un marco de certificación de ciberseguridad de la UE para productos y servicios TIC?

La certificación de seguridad de las TIC aumenta la confianza y la seguridad en los productos y servicios del mercado único digital. Ya existen algunas

[169] EUROPEAN UNION. (enero 2018). Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. The European Union Agency for Network and Information Security (ENISA). Recuperado de: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

certificaciones (*la Certificación Sécuritaire de Premier Niveau* en Francia, *Commercial Product Assurance* en el Reino Unido), pero estas generan barreras en contra del mercado único. Se intenta adaptar una regulación de forma individual con unos requisitos genéricos a cumplir. Los certificados resultantes que confirman el cumplimiento de tales requisitos se reconocen en todos los Estados miembros, lo que facilita a las empresas el transcomercio.Estos serán de uso voluntario para los agentes del mercado como ventaja competitiva, siendo muy útil para ciudadanos y usuarios finales (por ejemplo, operadores de servicios esenciales), que podrán tomar decisiones de compra más informadas relacionadas con los productos y servicios TIC en los que confían en el día a día. Los proveedores de productos y servicios de TIC tendrán que pasar por un único proceso para obtener un certificado europeo válido en todos los estados miembros y de esta forma eliminar barreras, abaratando el proceso para las empresas. Los gobiernos también podrán y deberán tomar decisiones de las áreas prioritarias que necesitan la certificación de seguridad de las TIC.

- ¿Cómo se integrará el marco europeo en iniciativas existentes o internacionales?

Las nuevas normativas creadas para la ciberseguridad ya en su creación han dependido de las normas internacionales y por ello no serán una barrera para el comercio interno de la UE ni para seguir operando con sus socios intentando que incorporen las medidas del marco Europeo.

- ¿Cuál es el propósito de la recomendación de una respuesta coordinada de la UE a los ciberataques (el Plan)?

Describe principios, mecanismos de gestión, entidades de ciberseguridad, mecanismos de cooperación y actores existentes en el campo de la ciberseguridad a nivel de la UE: recomendación de que la UE tenga un plan para ciberataque o crisis transfronteriza en gran escala; recomendación de tener objetivos y modos de cooperación entre los Estados miembros y las instituciones de la UE para responder a los ciberataques; y recomendación de solicitar a los Estados miembros y a las instituciones de la UE que establezcan una linea de respuesta ante crisis de ciberseguridad de la UE.

- ¿Qué cuerpos estarán involucrados en la gestión de las crisis? ¿Cómo se coordinarán?

Los siguientes organismos cooperarán juntos a nivel técnico, operativo y estratégico: Las autoridades nacionales competentes y los puntos únicos de contacto establecidos por la Directiva NIS; Los equipos de respuesta a incidentes de seguridad informática (CSIRT); ENISA y Europol / EC3 (el Centro Europeo de Ciberdelincuencia de Europol); La Comisión Europea; El Servicio Europeo de Acción Exterior.

- ¿Cómo se tratarán los ciberataques como *WannaCry* y (no) *Petya* según el *Blueprint*?

El objetivo del *Blueprint* es que la UE establezca un plan sólido y testeado para actuar ante un ciberincidente o crisis que implique cooperación a nivel europeo e internacional, por lo que es esencial la comunicación rápida entre actores y una respuesta coordinada. Además, hay que establecer mecanismos para identificar la causa de los ataques. Son los Estados miembros, con el mecanismo integrado de respuesta a la crisis política (IPCR), quienes dirán cuándo poner en marcha el plan.

- ¿Cuándo y por qué se establecerán la Red y el Centro europeo de investigación y competencia sobre ciberseguridad?

La UE necesita inversiones a gran escala en tecnologías, productos, procesos y conocimientos especializados en ciberseguridad.

Esto incluye la creación de una Red de Competencia de Ciberseguridad con un Centro Europeo de Investigación y Competencia de Ciberseguridad, y disponer de capacidad en este ámbito a escala nacional y de la UE.

La Comisión lanzará una evaluación de impacto para examinarlas. Establecerá esta estructura lo antes posible y propone una fase piloto bajo Horizon 2020 como nuevo impulso en ciberseguridad. También planea poner a disposición fondos de 50 millones de euros a corto plazo para esto.

- ¿Por qué desarrollar una respuesta eficaz en materia de derecho penal?

Hay que establecer unas medidas creíbles y disuasorias efectivas para los ciberdelincuentes y atacantes. La ley penal debe ser más eficaz ya que la respuesta de las fuerzas del orden se centra en la detección, trazabilidad y enjuiciamiento de los ciberdelincuentes.

La Directiva (2013) sobre ataques contra los sistemas de información establece normas mínimas sobre la definición de delitos y sanciones en el área de ataques contra los sistemas de información y proporciona medidas operativas para mejorar la cooperación entre las autoridades. Todavía debe alcanzar su máximo potencial y se requiere un mayor esfuerzo.

Se propone una nueva Directiva de lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo para proporcionar una respuesta más eficaz en materia penal al delito cibernético.

- ¿Qué es "fraude de pago no en efectivo"?

Aquellas acciones de estafa realizadas mediante los instrumentos de pago no monetarios más comunes que son las tarjetas de pago (crédito y débito), las transferencias de crédito, los débitos directos, el dinero electrónico, las monedas virtuales, el dinero móvil, los vales, los cupones y las tarjetas de fidelización. Las transacciones de pago no en efectivo han aumentado constantemente en Europa en los últimos años, tanto en términos de cantidad como de valor.

El fraude de pago no en efectivo puede tomar diferentes formas. Los delincuentes pueden desencadenar la ejecución de pagos utilizando la información del pagador obtenida a través de, por ejemplo, suplantación de identidad, robo u obtención de información en sitios web dedicados que venden credenciales de tarjetas de crédito robadas en la red oscura.

Los pagos pueden ejecutarse fraudulentamente mediante tarjetas falsificadas o robadas.

- ¿Por qué propone la Comisión una nueva Directiva sobre el fraude en los pagos no monetarios?

Por los cambios sustanciales en el área de pagos no monetarios y el aumento del fraude en línea. Se quiere garantizar que los crímenes cometidos con nuevos instrumentos de pago sean enjuiciados de manera efectiva, en el marco del derecho penal de la UE. Hay que actualizarse contínuamente para garantizar una aproximación del nivel de las sanciones.

Es necesario solucionar los problemas de territorialidad cometidos desde cualquier lugar, por lo que sería positivo la creación de un marco común de Derecho penal de la UE, en cuanto al fraude y la falsificación de medios de pago no monetarios para apoyar adecuadamente las investigaciones y procesamientos transfronterizos.

- ¿Cómo ayudará la nueva Directiva a luchar contra el fraude en el pago no en efectivo?

Siguiendo la línea y la estrategia de ciberseguridad de la UE con la nueva Directiva que reforzará la capacidad de los Estados miembros para enjuiciar y sancionar el fraude en pagos no monetarios se conseguirá fortaleciendo la capacidad de las autoridades contra este delito, ampliando el alcance de los delitos relacionados con los sistemas de información a todas las transacciones de pago, incluidas las transacciones a través de monedas virtuales. También ayudará con la introducción de normas comunes sobre las sanciones con un mínimo, pudiendo variar de dos a cinco años dependiendo de la ofensa.

La nueva legislación hace que sea un delito independiente poseer, vender, adquirir para su uso, importar o distribuir un instrumento de pago falsificado o falsificado robado o legalmente no apropiado.

Por otra parte hay que aclarar el alcance de la jurisdicción garantizándolo a los Estados miembros y garantizar que las víctimas de delito cibernético tengan derecho a acceder a información sobre asistencia y apoyo disponibles mejorando las condiciones para que las víctimas denuncien los delitos.

También es interesante la aplicación de las medidas prácticas para mejorar el acceso transfronterizo a las investigaciones penales sobre delincuencia electrónica y el desarrollo de una plataforma electrónica para intercambiar información dentro de la UE y la normalización de los formularios de cooperación judicial utilizados entre los Estados miembros.

La Comisión también está estudiando diferentes formas de reforzar las capacidades forenses en los Estados miembros. Un paso sería desarrollar aún más Europol y su Centro Europeo contra el Cibercrimen, para aumentar la capacidad de investigación contra la ciberdelincuencia, con un presupuesto de la UE que destinará 10,5 millones de euros en el marco del Fondo de Seguridad Interior (FSI).

- ¿Porqué fortalecer la cooperación internacional en seguridad cibernética?

La política internacional de ciberseguridad de la UE es evolutiva, global y cooperativa, aplicando el derecho internacional, y la Carta de las Naciones Unidas en el ciberespacio, buscando la estabilidad y la seguridad internacionales.

La UE tiene establecida la cooperación cibernética específica con los EE. UU., Japón, India, Corea del Sur y China y con asiduidad celebra consultas estrechas con organizaciones internacionales, como la OTAN, el Foro Regional de la ASEAN, la OSCE, el Consejo de Europa y la OCDE.

- ¿Cómo puede la UE responder diplomáticamente a actividades cibernéticas maliciosas?

El 19 de julio de 2017, el Consejo acordó las conclusiones sobre un marco para una respuesta diplomática conjunta a las actividades cibernéticas maliciosas (la "Caja de herramientas de ciberdelincuencia"). Esta permite a la UE prevenir y responder a actividades cibernéticas maliciosas, mediante el uso de medidas en el marco de los instrumentos de la Política Exterior y de Seguridad Común.

- ¿Cómo contribuirá la UE al desarrollo de la capacidad cibernética mundial?

La estabilidad cibernética mundial es un entramado basado en la capacidad local y nacional de todos los países que previene y reacciona ante los incidentes cibernéticos sirviendo para investigar y enjuiciar los ciberdelitos.

Desde el 2013, la UE ha liderado el desarrollo de la capacidad internacional de ciberseguridad, coordinando a la Comisión Europea y el Servicio Europeo de Acción Exterior con cada una de las autoridades cibernéticas de cada estado miembro. La UE pretende ayudar y ofrecer una mejor orientación política, priorización y optimización de esfuerzos a terceros países.

- ¿Por qué hay que cooperar en defensa cibernética?

Se necesita un rápido aumento de las capacidades de ciberdefensa dentro de la UE para mitigar el riesgo y responder adecuadamente a los ataques cibernéticos y hay iniciativas nuevas que es preciso tener en cuenta, como el Fondo Europeo de Defensa.

El Servicio Europeo de Acción Exterior y la Agencia Europea de Defensa (AED) se han comprometido en crear cooperación entre los Estados miembros desde 2013, cuando se creó el Equipo del proyecto de ciberdefensa AED.

Además, con las Políticas de Defensa Cibernética de la UE, adoptadas por la UE en 2014, se pretende aumentar la capacidad de los Estados miembros, racionalizar sus doctrinas, aumentar las oportunidades de formación y ejercicio, y promover la investigación, proteger la Política Común de Seguridad y Defensa misiones y operaciones, buscar sinergias civiles y militares enla UE y utilizar la investigación y el desarrollo de doble uso.

Los proyectos sobre ciberseguridad se basan en el marco de una cooperación estructurada permanente (PESCO).

- ¿Cómo se está desarrollando la cooperación UE-OTAN sobre ciberseguridad?

Según está previsto en la Declaración conjunta de 8 de julio de 2016sobre cooperación de la EU y OTAN en ciberseguridad, amenazas híbridas y defensa, estas intensificarán el intercambio de información entre sus respectivos órganos de ciberseguridad.

El equipo de respuesta ante emergencias informáticas para las instituciones de la UE (CERT-UE) y la capacidad de respuesta a incidentes informáticos de la OTAN (NCIRC), deben actuar de forma coordinada con paralelismo e

interoperando conjuntamente.

En relación a los esquemas de certificación existentes en la UE, actualmente, hay un mosaico de iniciativas y esquemas de certificación de ciberseguridad en Europa. Por un lado, las iniciativas nacionales de certificación ya están establecidas o están surgiendo sin reconocimiento mútuo. Por otro lado, no todos los Estados miembros de la UE son parte del principal mecanismo europeo basado en el reconocimiento mutuo (SOG-IS).

El *Commercial Product Assurance* (CPA) desarrollado en el Reino Unido se aplica a los productos comerciales a los que se otorgan certificaciones que demuestran buenas prácticas de seguridad comercial y certifican que un producto es adecuado para entornos de menor riesgo. Sin embargo, no existe un acuerdo de reconocimiento mutuo para CPA, lo que significa que los productos probados en el Reino Unido normalmente no se aceptarán como productos certificados en otros mercados.

La evaluación de productos de seguridad de línea de base holandesa (BSPA) proporciona información sobre la idoneidad de los productos de seguridad de TI para su uso en el dominio "sensible pero no clasificado". El esquema de BSPA ha estado en fase piloto desde 2015 y se espera que esté operativo a fines de 2017.

Por otra parte, hay otras iniciativas emergentes, como la certificación *Sécurité de Premier Niveau* (CSPN) que tieneun esquema de certificación de seguridad de TI establecido por la Agencia Nacional de Ciberseguridad de Francia (ANSSI). Al igual que el CPA, no existe un reconocimiento mutuo para CSPN, lo que significa que los productos probados en Francia normalmente no serán aceptados en otros mercados.

ElSOG-IS MRA[170] incluye 12 Estados miembros (Austria, Croacia, Estonia, Finlandia, Francia, Alemania, Italia, Países Bajos, Luxemburgo, Noruega, Polonia, España, Suecia, Reino Unido) y ha desarrollado algunos perfiles de protección en productos digitales, p. ej., firma digital, tacógrafo digital y tarjetas

[170] Vid. *Senior Officials Group Information Systems Security (SOG-IS) <https://www.sogis.org/>*

inteligentes. Los miembros pueden participar en acuerdos de reconocimiento mútuo decertificados de consumidores y productores" *(traducción propia*)[171].

f) Decisiones de calado de la Unión Europea en Ciberseguridad

- Intensificar la capacidad de ciberseguridad de la UE:

El interés estratégico de la UE está relacionado con el desarrollo de herramientas tecnológicas de seguridad cibernética y la protección de hardware y software crítico. Esto permitirá el florecimiento de la economía digital, nuestra seguridad y el respeto a la democracia.

- Un Centro Europeo de Investigación y Competencia de la Ciberseguridad:

Se establecerá una prueba piloto en 2018 para garantizar que nuestras defensas sean tan avanzadas como las armas que utilizan los ciberdelincuentes.

Complementará los esfuerzos de creación de capacidad en ciberseguridad a escala nacional y de la UE.

- Un proyecto de cómo Europa y los Estados miembros pueden responder de manera rápida:

De forma operativa y al unísono. La Recomendación también pide a los Estados miembros y a las instituciones de la UE que establezcan un plan de respuesta ante una crisis de ciberseguridad en la UE. Para que el plan sea operativo debe probarse regularmente.

- Más solidaridad:

Un Fondo de respuesta para incidentes en ciberseguridad, para los Estados miembros que cumplan todas las medidas de ciberseguridad exigidas por la legislación de la UE.

- Mayor capacidad de ciberdefensa:

Los estados deben incluir la ciberdefensa en el marco de la cooperación

[171] Vid.EUROPEAN COMMISSION. (2017). Ob., cit., p. 2.

estructurada permanente (PESCO) y el Fondo Europeo de Defensa para apoyar proyectos de defensa cibernética.

El Centro Europeo de Investigación y Competencia en Ciberseguridad también podría desarrollarse aún más con una dimensión de ciberdefensa.

La UE creará una plataforma de educación y capacitación en defensa cibernética en 2018.

La UE y la OTAN incrementaran su cooperación e impulsarán conjuntamente la investigación en ciberdefensa e innovación realizando ejercicios conjuntos.

- Cooperación internacional reforzada:

La UE reforzará su respuesta a los ciberataques implementando más cooperación entre los estados miembros y ayudando a terceros países a abordar las amenazas cibernéticas.

- Crear una respuesta efectiva de derecho penal:

Una respuesta efectiva de las fuerzas de seguridad, centrada en la detección, la rastreabilidad y el enjuiciamiento de los ciberdelincuentes. La ley introducirá normas comunes sobre el nivel de las penas y aclarará el alcance de la jurisdicción de los Estados miembros en dichos delitos.

En octubre de 2017 la Comisión presentó sus reflexiones sobre el papel de Encriptación en investigaciones criminales y expondrá sus propuestas para facilitar el acceso transfronterizo a pruebas electrónicas en 2018.

g) Resumen de datos genéricos de la UE en Ciberseguridad

- Resistencia, disuasión y defensa: construir una ciberseguridad sólida en Europa:

La estrategia de la UE y en particular de sus dirigentes, la Comisión y sus altos representantes es la de estar preparados contra los desafíos en ciberseguridad, a través de una estrecha cooperación de sus estados miembros

en todas sus estructuras implicadas.

- Los ciudadanos y las empresas europeas confían en los servicios y las tecnologías digitales:

¿Cómo piensan los europeos que afecta positivamente las nuevas tecnologías sobre su hábitat?: El 75% en nuestra economía; El 64% en nuestra sociedad; El 67% en muestra calidad de vida; El 86% de los europeos creen que la posibilidad de ser víctimas del ciberdelito ha aumentado considerablemente porque la mayoría de los sectores dependen de las nuevas tecnologías.

- Evolución de los ciberincidentes:

Más de 4.000 ataques ransonware por dia en 2016, el80% de las empresas tuvieron algún ciberincidente en 2016, un 35% de aumento en ciberincidentes del 2015 al 2016: el mayor en 12 años, y más de150 países y 230.000 sistemas fueron afectados en 2016 en todos los servicios, incluso hospitales.

Los ataques de ransomware han aumentado en un 300% desde 2015, el impacto económico del cibercrimen se multiplicó por 5 entre 2013 y 2017, y podría aumentar cuatro veces más en 2019.

Además, entre las principales amenazas a la seguridad nacional ya están los ataques cibernéticos de otros países y la economía mundial estima que un ciberataque importante podría costarle 100 millones de euros.

- Actuaciones de los ciudadanos europeos:

El 45% ha instalado un software antivirus, el 62% ha cambiado sus contraseñas en los últimos 6 meses. El 12% ha reducido sus compras en línea y el 10% ha optado por abandonar la banca en línea.

- La actitud a seguir por la Unión Europea:

Todas las medidas y actitudes de la UE a pesar de ser multitudinarias todavía son insuficientes: el 51% de los ciudadanos no está bien informado de las consecuencias de los ciberdelitos; un 60% de las empresas nunca han estimado los gastos que los ciberataques pueden ocasionarles; y el 69% de las empresas no sabe a lo que se expone.

"Este amplio paquete de seguridad cibernética se basa en instrumentos existentes y presenta nuevas iniciativas para mejorar aún más la ciberresistencia y la respuesta de la UE en tres áreas clave: Desarrollar la resiliencia de la UE frente a ciberataques y aumentar la capacidad de ciberseguridad de la UE. Crear una respuesta de derecho penal efectiva a través de la cooperación internacional".

"Hechos y cifras: La escala del problema hace que la necesidad de actuar sea aún más urgente. Las cifras recientes muestran que las amenazas digitales están evolucionando rápidamente: desde el comienzo de 2016, se han producido más de 4.000 ataques de ransomware en todo el mundo, un aumento del 300% desde 2015, mientras que el 80% de las empresas europeas se han visto afectadas el año pasado. Los estudios sugieren que el impacto económico del delito cibernético se quintuplicó entre 2013 y 2017, y podría aumentar aún más en un factor de cuatro en 2019. El ransomware ha experimentado un aumento particular, con los recientes ataques reflejando un incremento dramático en la actividad del ciberdelito. Sin embargo, ransomware está lejos de ser la única amenaza" (*traducción propia)*[172].

II.5.- DEFENSA DE LA UNIÓN EUROPEA ANTE LOS ATAQUES CIBERNÉTICOS

Se necesitan estructuras más sólidas y eficaces para ciberdefenderse, además de una organización y actuación de forma conjunta con las más modernas tecnologías.Pasos a seguir:

- Desarrollar una defensa de la UE frente a ciberataques y reforzar la capacidad de ciberseguridad de la UE.
- Crear una legislación y respuesta penal efectiva.
- Fortalecer la estabilidad global mediante el continuo desarrollo de la cooperación.

[172] Vid.EUROPEAN COMMISSION. (19 de septiembre de 2017b). Fact sheet: The Commission scales up its response to cyberattacks. Pag. 1, Brussels.

En consecuencia, la Comisión y sus representantes: proponen reforzar ladefensa, la disuasión y la respuesta de la UE a los ciberataques mediante:

- "El establecimiento de una Agencia de Ciberseguridad de la Unión Europea más sólida, basada en la Agencia para la Seguridad de las Redes y la Información (ENISA), para ayudar a los Estados Miembros a enfrentar los ciberataques.
- La creación de un esquema de certificación de ciberseguridad en toda la UE que aumente la ciberseguridad de productos y servicios en el mundo digital.
- Un modus esterotipo sobre cómo responder de manera rápida, operativa y al unísono cuando ocurre un ciberataque a gran escala.
- Una red de centros de competencia en los Estados miembros y un Centro Europeo de Investigación y Competencia en Ciberseguridad, que ayudará a desarrollar y desplegar las herramientas y la tecnología necesarias para mantenerse al día, con una amenaza en constante cambio y garantizar que nuestra defensa sea lo más fuerte posible.
- Una nueva Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, para proporcionar una respuesta más eficaz en materia penal, a los delitos cibernéticos.
- Un marco para una respuesta diplomática conjunta de la UE, a actividades cibernéticas maliciosas y medidas para fortalecer la cooperación internacional en ciberseguridad, incluída la profundización de la cooperación entre la UE y la OTAN.
- La UE tiene como objetivo, impulsar el desarrollo de habilidades de alto nivel para profesionales civiles y militares, a través de la provisión de soluciones para los esfuerzos nacionales y la creación de una plataforma educativa y de capacitación en defensa cibernética"*(Traducción propia)*[173].

[173] JUNCKER, J-C. (13 September 2017). Ob., cit., p. 2.

II.6.- ACTUALIDAD EN MATERIA DE TERRORISMO EN LA UNIÓN EUROPEA

La comisión Europea ha presentado su cuarto informes obre los progresos realizados en la construcción de una Unión de Seguridad eficaz y auténtica (*Fourth progress report towards an effective and genuine Security Union*)[174]. El informe de 2017"destaca los principales acontecimientos en cuatro ámbitos: i) los sistemas de información y la interoperabilidad; ii) la protección de objetivos suaves; iii) la amenaza cibernética; y iv) la protección de datos en el contexto de las investigaciones penales. El informe también describe algunas de las próximas iniciativas encaminadas a fortalecer aún más la defensa y resiliencia de la UE contra el terrorismo y la delincuencia organizada. El Comisario europeo de la Unión de Seguridad, JULIAN KING, declaró que: Es esencial que continuemos nuestro importante trabajo para conectar y mejorar nuestras bases de datos y el intercambio de información, ya que esto marcará una verdadera diferencia para la seguridad de Europa. Necesitamos dedicar un esfuerzo adicional a la construcción de nuestra capacidad de resistencia en el ciberespacio, a la lucha contra el delito cibernético, a la inversión en investigación e innovación en este ámbito ya una cooperación amplia con la industria, los Estados miembros y terceros países. Debemos dentificar nuevas medidas para proporcionar un marco eficaz a escala de la UE para la seguridad cibernética"[175].

En definitiva los países (como hemos podido observar analizando a los diferentes autores y sus estudios sobre terrorismo), están llevando a cabo un planteamiento de defensa con unas líneas tanto individuales (dentro de sus fronteras) como colectivas (fuera de éstas). Se está desarrollando una red de cooperación internacional cada vez más grande, donde los países, en función de sus intereses estratégicos y situación geográfica interactúan en un mayor o menor grado; donde sus cuerpos de seguridad e inteligencia interaccionan entre ellos y

[174] EUROPEAN COMMISSION. (25 de enero de 2017). Fourth progress report towards an effective and genuine Security Union. Recupearo de: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20170125_4th_progress_report_on_the_security_union_en.pdf

[175] CENTRO DE ANÁLSIS Y PROSPECTIVA, GUARDIA CIVIL. (enero de 2016). *Boletín UE*. CAP, p. 6. Recuperado de: http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/17619.pdf

donde además de compartir medios tanto tecnológicos como humanos, sobre todo se comparte lo más valioso de nuestra era: "la información". Este manejo de información es lo que les da una ventaja contra las organizaciones delictivas y permite poder combatir como primer objetivo esta nueva epidemia del siglo XXI: el terrorismo".

Dentro del marco de la cooperación europea resaltamos la siguiente documentación, agencias e instituciones de la UE[176]:

- EUROPOL, Oficina Europea de Policía: "*Ramsomware*: Lo que usted necesita saber" (informe conjunto de *Check Point* y Europol); infografía. *Spyware.*

- OEDT. Observatorio Europeo de Drogas y Toxicomanías. Reducción de la oferta de drogas: panorama de las políticas y medidas de la UE. Sanciones contra el tráfico de drogas en toda la Unión Europea: un estudio de la opinión de expertos.

- EUROSTAT, Oficina de Estadística de la Unión Europea. Cifras clave de Europa - edición 2016.

- ENISA, Agencia Europea de Seguridad de las Redes y de la Información (directrices para las PYME sobre la seguridad del tratamiento de los datos personales; seguridad cibernética y Resistencia de los coches inteligentes).

- Directrices para las PYME sobre la seguridad del tratamiento de los datos personales. Seguridad cibernética y resistencia de los coches inteligentes

- EPRS, Servicio de Investigación Parlamentaria Europea. Diez temas para seguir en 2017. Paquete de ampliación 2016: Perspectivas para los Balcanes Occidentales. Políticas de igualdad de género en España: actualización. Bienestar animal en la Unión Europea. Relaciones entre los Estados miembros de la UE y Arabia Saudita en el ámbito de la seguridad y la defensa. Elecciones de 2016 en los Estados Unidos: efectos sobre la relación UE-EE.UU. Control de la adquisición y posesión de armas. Violencia sexual contra menores en América Latina. Condiciones

[176] Ibídem., p. 34.

penitenciarias en los Estados miembros: Selección de normas y buenas prácticas. Procedimiento común de asilo de un vistazo. Derechos humanos en Filipinas.

- Ejecución del plan general de lucha contra el terrorismo establecido por el Consejo Europeo (informe sobre los avances realizados en el marco de las conclusiones sobre la lucha antiterrorista en febrero de 2015).
- Informe anual del Tribunal Europeo de Derechos Humanos.
- Informe anual sobre el Plan de Acción Regional del Sahel.
- Plan de acción para reforzar la respuesta europea contra la falsificación de los documentos de viaje.
- Mecanismo de Protección Civil de la Unión: la coordinación de las respuestas a los desastres fuera de la UE ha sido ampliamente eficaz.
- Tratados consolidados, Carta de los Derechos Fundamentales (2016).
- Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica.
- Directrices sobre la protección de las personas en relación con el tratamiento de datos personales en un mundo de Big Data"[177].

El intercambio de información en la lucha contra el terrorismo alcanza un máximo histórico.

"Europa se enfrenta a su más grave amenaza terrorista durante más de 10 años. Los ataques a *Charlie Hebdo*, en enero de 2015 marcaron un cambio hacia una estrategia más amplia del terrorismo yihadista, y el objetivo de la llamada es, en particular, intimidar a los países occidentales con sucesivos ataques terroristas en toda Europa. El aumento potencial de los retornados de las zonas de conflicto requiere vigilancia por parte de todos los actores involucrados.

[177] Ibídem., pp. 34-46.

El lanzamiento de la Centro Europeo Contraterrorista[178] (ECTC, sus siglas eninglés) en enero de 2016 fue la respuesta de la UE a esta nueva amenaza. Su creación, incluyendo la Unidad de referencia de Internet (IRU) como una nueva capacidad para hacer frente a niveles sin precedentes de la propaganda terrorista en línea, fue un hito importante para la arquitectura de seguridad de la UE. Por primera vez en la UE había consenso, en el contexto de la política de lucha contra el terrorismo, que necesitaba una piedra angular de la cooperación a nivel de la UE para apoyar los esfuerzos nacionales de lucha contra el terrorismo.

El intercambio de información sobre lucha contra el terrorismo, en todos los países europeos, así como a través y con Europol, había llegado a su punto más alto a finales de 2016. Por ejemplo, Europol llevó a cabo 10 veces más información sobre la persona 'entidades' en su base de datos, en comparación con enero de 2015, cuando se llevó a cabo el ataque a *Charlie Hebdo*.

La función como centro de intercambio de información, realización de análisis y coordinacióndel apoyo operativo está siendo explotada por los Estados miembros de la UE y terceros relevantes, lo que indica un aumento significativo en la confianza y el conocimiento a través de las autoridades nacionales de lucha contra el terrorismo en relación con los servicios de apoyo de Europol"[179].

II.6.1.- Actualidad de la Unión Europea en seguridad, terrorismo y defensa

Bruselas redobla esfuerzos para evitar la radicalización terrorista de los ciudadanos comunitarios. Así la Comisión Europea (CE) ha destacado la puesta en marcha de un proyecto para evitar la radicalización de personas con pasaporte europeo. La iniciativa se denomina Programa de Fortalecimiento de la Sociedad Civil, nace en marzo de 2017 y tiene el objetivo de prevenir y luchar contra la radicalización de ciudadanos nacionales europeos dentro del suelo de la Unión, basándonos en la información que facilita el comisariado europeo[180].

[178] PRESS DIGITAL. (25 enero de 2016). Europol alerta de que los terroristas del Estado Islámico pueden volver a atentar en Europa. Recuperado de: https://www.pressdigital.es/texto-diario/mostrar/398663/europol-alerta-terroristas-estado-islamico-pueden-volver-atentar-europa

[179] CENTRO DE ANÁLSIS Y PROSPECTIVA, GUARDIA CIVIL. (enero de 2016). Ob., cit., p. 6.

[180] COM(2017) 213 final, Bruselas 21 de abril de 2017.

Por su parte, JULIAN KING, comisario de Seguridad de la UE afirmó que "este informe proporciona un sólido fundamento sobre el que debatir como prioridad en la UE durante los próximos cuatro años para reducirel espacio en el que terroristas y grupos de crimen organizado operan"[181].

La principal amenaza son los terroristas individuales o grupos individuales compuestos por 1, 2, 3 ó 4 individuos que normalmente tienen pasaporte comunitario y que alguno de ellos ha sido formado militarmente en alguno de los conflictos en los que participa el DAESH, y que vuelve a territorio europeo o bien para utilizar esta formación o trasmitirla a otros seguidores. Ahora mismo uno de los principales objetivos de las fuerzas de seguridad europeas es controlar este tipo de migración radicalizada ya que es el origen de la mayoría de los atentados producidos últimamente en territorio Occidental.

Como segundo punto de actualidad, la UE refuerza el control de la adquisición y tenencia de armas de fuego[182], asi la línea futura a seguir por los países de la Unión Europea es el control, seguimiento y localización de las armas de fuego dentro de sus fronteras.

"El 25 de abril de 2017, el Consejo ha adoptado una Directiva sobre el control de la adquisición y tenencia de armas, que revisa y completa la Directiva 91/477/CEE existente"[183].

La estrategia que quiere seguir Europa consiste en una revisión exhaustiva de las armas así como su marcado llevando ésto a un mejor control de éstas, así como una inutilización de éstas cuando dejen de cumplir la normativa o dejen de utilizarse.

De esta forma, por ejemplo, unas normas más estrictas para la adquisición y tenencia de armas de fuego y limitación de armas de tipo A (incluyendo aquí ciertas armas semiautomáticas o largas de fácil ocultación consideradas muy

[181] CENTRO DE ANÁLSIS Y PROSPECTIVA, GUARDIA CIVIL. (abril de 2017). Boletín UE. CAP, p.5. Recuperado de: http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/documents/19610_20840.pdf

[182] Ibídem., p. 6.

[183] CONSEJO UNIÓN EUROPEA. (25 de abril de 2017). Directiva sobre el control de la adquisición y tenencia de armas, que revisa y completa la Directiva 91/477/CEE. Recuperado de: http://www.consilium.europa.eu/es/press/press-releases/2017/04/25/control-acquisition-possession-weapons/

peligrosas) a determinados grupos de la población;y sobre todo facilitar, agilizar y promover el intercambio de información por medios electrónicos entre las fuerzas de seguridad de los estados miembros.

Estrategias internacionales de España en la Unión Europea

Se han producido diversos tratados de cooperación con grandes zonas antes incontrolables por su extensión y su poca colaboración, que servían de refugio a todo tipo de criminales. Europol ha firmado con China un tratado de cooperación para luchar contra el crimen.

"La firma del Acuerdo de Cooperación Estratégica concluye con éxito las negociaciones entre la República Popular de China y Europol sobre cómo unir efectivamente fuerzas para luchar contra la delincuencia grave y organizada. Tras la entrada en vigor del acuerdo, este nuevo nivel de cooperación será importante para abordar ámbitos delictivos prioritarios que afectan tanto a la Unión Europea como a China"[184].

Se reabre de nuevo por parte de Estados Unidos la alerta de viaje a Europa por la "continua amenaza terrorista".

"El Gobierno de Estados Unidos emitió este mes de mayo una alerta de viaje en la que avisa a sus ciudadanos que "continúa la amenaza terrorista" en Europa, al considerar que el Estado Islámico (EI) ha demostrado su "capacidad" de perpetrar atentados en varios de esos países.

"Los recientes incidentes en Francia, Rusia, Suecia y el Reino Unido demuestran que el EI, Al Qaeda y sus filiales tienen la capacidad de planear y ejecutar ataques terroristas en Europa", indica una alerta de viaje emitida por el Departamento de Estado de Estados Unidos, que estará en vigor hasta el 1 de septiembre de este año"[185] (2017).

La línea de los Estados Unidos es proteger sus fronteras desde dentro o fuera de ellas e intenta evitar cualquier contagio de brotes sobre todo, organizados

[184] CENTRO DE ANÁLSIS Y PROSPECTIVA, GUARDIA CIVIL. (abril de 2017). Ob., cit., p. 7.
[185] Ibídem., p. 9.

por terroristas. Observa los últimos atentados en Europa y quiere advertir a su población de ésto e intentar evitar que se traslade a su territorio decidiendo también aumentarotra vez el control de sus fronteras en el tráfico aéreo proveniente de Europa.

Otro fenómeno que crece en tamaño y preocupación es el fenómeno de los ciberataques provenientes de Corea del Norte:

"La principal agencia de espionaje de Corea del Norte tiene una céluda especial denominada Unidad 180 que es probable que haya lanzado algunos de sus ciberataques más audaces y exitosos, según desertores, funcionarios y expertos en seguridad de Internet" (Traducción propia del texto)[186]*.*

Los servicios de seguridad del mundo centran gran parte de su atención sobre un país cuyos movimientos cibernéticos son desconocidos para los occidentales y que además de ser una amenaza nuclear para el mundo, también es una gran amenaza para el ciberespacio mundial debido a las malas praxis y ataques que según los servicios de inteligencia provienen de allí.

II.6.2.- Ciberseguridad, Internet y protección de datos

"*No more Ransom*" añade 15 nuevas aplicaciones y suma nuevos socios: Después de los ataques que infectaron a millones de usuarios gran cantidad de policías y socios privados se han adherido a la iniciativa "*No more Ransom (NMR)*" poniendo operativas 15 nuevas herramientas que pueden facilitar el descifrado a miles de usuarios.

La plataforma <*www.nomoreransom.org*> está disponible en 14 idiomas y contiene 40 herramientas de descifrado libres. Desde su publicación el pasado diciembre, más de 10.000 víctimas de todo el mundo han sido capaces de descifrar sus dispositivos afectados gracias a las herramientas disponibles de forma gratuita

[186] *ABC NEWS.* (21 de Mayo de 2017).North Korea's Unit 180, the cyber warfare cell that worries the West*, Australia.* Recuperado de: http://www.abc.net.au/news/2017-05-21/north-koreas-unit-180-cyber-warfare-cell-hacking/8545106

en la plataforma"[187].

Según PANIAGUA (2017), en el caso concreto de España podemos ver claramente que los políticos andan a oscuras. "Conectividad, emprendimiento, I+D+i, industria 4.0, Mercado Único Digital (MUD), privacidad, protección de datos y seguridad; digitalización judicial, sanitaria, educativa y de la Administración; ciudades inteligentes, plataformas... Son algunos de los puntos a abordar en una Agenda Digital intensiva. ¿Cuáles son las líneas estratégicas de los respectivos grupos parlamentarios para desarrollarla? Es la pregunta planteada por la consultora *Kreab* en un encuentro con representantes del PP, PSOE y Ciudadanos".

"Si algo queda claro es que esas líneas estratégicas no están claras, ni las prioridades son las mismas para unos y para otros, a pesar de que, como señala el secretario sectorial de Nuevas Tecnologías del PP VÍCTOR CALVO-SOTELO, es un ámbito donde no hay puntos de enfrentamiento significativo. En su opinión, lo más importante desde el mundo público es lograr que, a nivel social, el país busque situar a España en una posición de excelencia. Y para ello, el también ex secretario de Estado de Telecomunicaciones y Sociedad de la Información cree fundamental que desde la política se promocione la importancia de los retos digitales"[188].

"Está de acuerdo con ello ÓSCAR GALEANO, portavoz de Agenda Digital del Grupo Socialista en el Congreso de los Diputados, que culpa al Gobierno de no asumir con suficiente convencimiento esa labor de concienciación ciudadana y empresarial: Consideramos que la digitalización ofrece a la ciudadanía una oportunidad pero, tal y como está planteada, puede generar riesgos, incertidumbres y rechazos, muchas veces por desconocimiento de las oportunidades asociadas a la transformación digital, afirma"[189].

En relación a la "regulación y formación especializada: El portavoz del PSOE insiste en la importancia de adaptar una legislación en algunos casos analógica al mundo digital para dotar de certidumbre al mundo empresarial y

[187] CENTRO DE ANÁLSIS Y PROSPECTIVA, GUARDIA CIVIL. (abril de 2017). Ob., cit., p. 10.

[188] PANIAGUA, E. (19 de mayo de 2017). Los políticos, perdidos ante la era digital. *El Mundo.* Economía, España. Recuperado de: http://www.elmundo.es/economia/2017/05/19/591e0a97ca4741a93d8b45c8.html

[189] Ibídem.

ciudadano. Lo que no está tan claro es cómo hacerlo. Es necesario formar a los parlamentarios porque cada uno venimos de una rama y el mundo digital es muy amplio", comenta. Propone crear un comité de expertos donde debatir con el objetivo de llegar a un equilibrio para avanzar, en lugar de generar trabas al desarrollo tecnológico. CALVO SOTELO coincide en la necesidad de que los grupos parlamentarios se especialicen porque muchas cuestiones de este sector tienen una complejidad técnica"[190].

Es evidente que los ciberterroristas y atacantes cibernéticos se aprovechan de esta falta de consenso legal teórico y operativo, muchas veces creada u olvidada por falta de inteligencia cibernética política, ya que éstos son los encargados de promover y actualizar las leyes que defiendan al usuario.

Cada vez más grupos terroristas tienen clara su estrategia de propagación. El desarrollo publicitario de sus organizaciones es exponencial, quieren llegar a sus adeptos de todo el mundo y crear más que todavía no lo son, pero sobre todo su objetivo se centra en aquellos residentes en territorio occidental. De esta forma adhieren mas poder operativo y destructivo a la organización.

"El 10 y 11 de abril de 2017, el Centro Europeo de lucha contra el Terrorismo de Europol (ECCT) organizó su primera Conferencia de alto nivel sobre propaganda terrorista en línea. En esta ocasión, más de 150 participantes se reunieron en la sede de Europol en La Haya para discutir una amplia variedad de temas relacionados con la amenaza terrorista en línea. Entre los participantes había miembros del Grupo Asesor ECTC en propaganda terrorista, representantes de la Comisión y del Consejo de la UE, el mundo académico y agentes profesionales de Europa y EE.UU."[191].

Las fuerzas de seguridad de todos los países occidentales y orientales afectados por la lacra del terrorismo lo saben y tratan de contrarrestar sus efectos[192]. Mr. GUNN WEIMANN, director del Centro Antiterrorista Europeo de Europol, disertó sobreeste fenómeno en concreto y mostró información de

[190] Ibídem.

[191] Europol acoge una conferencia sobre la propaganda terrorista en línea. Vid.CENTRO DE ANÁLISIS Y PROSPECTIVA, GUARDIA CIVIL. (abril de 2017). Ob., cit., pp.10-11.

[192] Este ha sido uno de los puntos debatidos en el congreso del pasado mes de Junio de 2017 (14-15) en Madrid-Aranjuez "*New Approaches on Fighting Security Threats*".

diferentes organizaciones terroristas (DAESH y Al Qaeda): sus logotipos, campañas de promoción e incluso comentó sus estrategias de forma estudiada y estructurada. También se tratóla posible competencia a la hora de la captación y dirección de la lucha terrorista por parte de las organizaciones terroristas en cuestión.

II.6.3.- *Atentados de Manchester y Londres: Gran Impacto social*

Todos los atentados terroristas son de gran impacto social, y por supuesto hacen estremecer la confianza de los ciudadanos de la Unión Europea, hasta el punto que la mayoría de los críticos coinciden que estos últimos atentados de la ciudad de Manchester y Londres (2017) han causado grandes grietas en la base de la defensa antiterrorista de los países occidentales han creado un gran debate sobre la organización de la estructura del sistema legal de las naciones civilizadas. Siempre se había defendido de forma abrumadora anteponer la defensa de los derechos fundamentales a la intimidad y anteponer la presunción de inocencia frente a la seguridad de los ciudadanos.

"Un atentado suicida cometido este lunes en Manchester (22-05-2017) *al término del concierto de la cantante estadounidense ARIANA GRANDE ha dejado un balance provisional de 22 muertos y 59 heridos. El ataque fue perpetrado a las 22.35, cuando los asistentes al concierto, la mayoría menores de edad, abandonaban el pabellón Manchester Arena"*[193]*.*

Muchos políticos y por supuesto la masa de los ciudadanos están empezando a tener dudas y ya se está hablando de posibles cambios en las legislaciones que permitan disminuir estos derechos a favor de incrementar la seguridad de las infraestructuras y personas sobre todo de estas últimas.

Horas después del atentado de Londres (03-06-2017) la primera ministra británica THERESA MAY[194] proclamó ante los medios de comunicación que: "Las

[193] *EL PAÍS.* (24 de mayo de 2017)Así te hemos contado el atentado en el Manchester Arena.España. Recuperado de: https://internacional.elpais.com/internacional/2017/05/23/actualidad/1495496576_039320.html

[194] DIARIO POPULAR. (4 de junio de 2017). Discurso Primera Ministra Británica. Recuperado de: https://www.diariopopular.com.ar/internacionales/theresa-may-pidio-leyes-mas-duras-contra-el-

cosas tienen que cambiar".

Se facilitarán todos los poderes que necesiten las fuerzas de seguridad para regular el ciberespacio y en definitiva los actos terroristas.

Se creará un mecanismo de control, actualización y estandarización de las leyes contra los delitos cibernéticos. La base de la lucha contra el terrorismo, está en el control del ciberespacio.

"La primera ministra advirtió que las operaciones antiterroristas o militares no son suficientes para acabar con los atentados o derrotar a esa ideología: "Sólo será derrotada cuando cambiemos la mentalidad de la gente sobre la violencia y les hagamos comprender que nuestros valores (los valores pluralistas británicos) son superiores a cualquier cosa que ofrezcan los predicadores del odio".

Su segundo argumento consistió en decir que se necesitan acuerdos internacionales para "acabar con ese espacio seguro (online) que el extremismo necesita para crecer" y que facilitan las grandes empresas de internet.

En tercer lugar, y esto supone un gran cambio, dijo que esa batalla contra los "espacios seguros" no debe realizarse sólo en el mundo digital, sino también en el mundo real: "Por eso, debemos ser más fuertes en identificarlos y borrarlos del sector público y de la sociedad. Eso exige un debate difícil y a menudo embarazoso".

Su último punto fue confirmar una revisión de la estrategia antiterrorista que se ha venido aplicandodesde noviembre de 2016 y que se ampliará para aumentar las penas de prisión para delitos relacionados con el terrorismo, incluso si implican delitos menos graves.

Es más probable que MAY apueste por penas mayores para delitos menos graves, como los relacionados con drogas o evasión fiscal, con los que procesar a sospechosos de terrorismo, en vez de resucitar el uso de órdenes como las

terrorismo-n311117

Tpims (medidas contra sospechosos ordenadas por el Ministerio de Interior)"[195].

Habló también acerca de las posibles estrategias para sino derrotar, aminorar al máximo este fenómeno terrorista que tanto daño ha hecho últimamente en el mundo y concretamente en la sociedad Británica.

- MAY explica cuatro líneas de combate contra el *terrorismo:* La lucha debe ir dirigida a arrasar la ideología: se pretende atacar directamente sobre el comportamiento adulterado, criminal y radical de los Yihadistas y nunca contra la idea real y pacífica del Islam.

- El mundo necesita una nueva y más fuerte regulación del ciberespacio, más estricta, organizada, estandarizada y sobre todo que cubra la totalidad del espacio cibernético.

- Menos tolerancia: las naciones que sufran esa lacra terrorista no pueden ir con contemplaciones; deben de actuar con autoridad y unidas contra el enemigo común terrorista.

- Revisar estrategias de lucha: no se trata de revisar específica o puntualmente la estrategia de lucha antiterrorista. Esta se debe revisar continuamente de forma organizada y estandarizada para todos los países.

Todos estos nuevos datos confirman varias conclusiones de nuestra Tesis: Si se siguen produciendo atentados se tomarán futuras medidas de tipo legal-legislativo para facilitar a las fuerzas de seguridad el éxito en sus actuaciones.

II.6.4.- Congreso "New approaches on fighting security threats"

Los pasados 14 y 15 de junio del 2017 se celebró en Madrid-Aranjuez el congreso internacional de aproximación entre países sobre las estrategias seguidas por estos en seguridad cibernética y concretamente ciberterrorista[196]. De la asistencia

[195] TRAVIS, A. (4 de junio de 2017). THERESA MAY recupera su discurso contra el extremismo que hasta ahora no había aplicado en el Gobierno, *The Guardian*, *www.eldiario.es*, Londres. Recuperado de: http://www.eldiario.es/theguardian/atentado-Londres-May_0_650935283.html

[196] El Centro Universitario de la Guardia Civil (CUGC) organizó el Congreso Internacional "Innovaciones tecnológicas y legales en la UE contra las amenazas a la seguridad" en colaboración con la Comisión Europea en el desarrollo de proyectos de fortalecimiento institucional y estabilidad

al congreso se pueden extraer algunas ideas.

El primer ponente fue PETER KRANJNYAK, responsable jefe del proyecto EU/MENA/CEPOL explicó que esta entidad busca la unidad tanto en formación, tecnología y estandarización de los proyectos de seguridad de la Unión Europea[197].

A continuación, LANGOU, Jefe del proyecto NEOGEND de la Gendarmería Nacional Francesa, nos explicó cómo funciona este proyecto, detallando que consiste en un portal-web de comunicación interna policial y de información rápida, efectiva y directa al ciudadano; donde el ciudadano puede denunciar y recibir respuesta de manera instantánea para cualquier tipo de delito y más en concreto para la investigación de cualquier indicio que permita evitar ataques de índole terrorista.

El Teniente Coronel MARIO LA MURA, ponente 3º, perteneciente al cuerpo de carabineros italianos destinado en Madrid, nos detalló el funcionamiento del software Italiano que utilizan sus unidades y que facilita el intercambio de información entre agentes. El programa busca la máxima rapidez y operatividad de respuesta, su nombre es ODINO (*Operational Device for Information Networking and Observation*).

Seguidamente, EMILIO VERÓN especialistay Jefe del departamento de Ciencias Forenses del Centro Universitario de la Guardia Civil (CUGC), se encargó de explicar el *modus operandi* y organigrama de esta tarea dentro del servicio de la Guardia Civil, así como detallarnos las unidades y capacidades disponibles.

TIZIANA LIGUORI fue la que abrió más tarde el debate sobre la Inmigración detallando la situación actual en las fronteras italianas del mar Mediterráneo y trató el problema general de la entrada ilegal de personas en la Unión Europea. También, PAOLO SALIERI, jefe de la oficina de inmigración y asuntos internos, relatóla situación, estrategias y logros actuales en inmigración de la Unión

en nuestras fronteras exteriores y otros escenarios geopolíticos, con el objetivo de romover el conocimiento de experiencias del Espacio Europeo de Educación Superior (EEES) en materia de tecnología y seguridad, en las fronteras exteriores de la UE. Vid. Más información en: https://www.cugc.es/extension-universitaria/actividad-internacional/item/36-innovaciones-tecnologicas-taiex-2017

[197] Vid. www.cepol.europa.eu

Europea.

Siguiendo con el tema de la Inmigración, el Comandante operativo IGOR DE LA CASA, de la Jefatura de Fiscal y Fronteras de la Guardia Civil, detalló la situación actual en materia fiscal e inmigración en las fronteras españolas, más concretamente el tráfico de drogas y tráfico de personas en el sur de España.

La segunda jornada del Congreso empezó en el Salón de actos recientemente inaugurado delcomplejo académico y universitario de la Guardia Civil en Aranjuez con la participación de FRANCOIS-XAVIER MASSON Jefe de la unidad contra el delito tecnológico y terrorismo organizado de Francia, que informó del funcionamiento de esta unidad y del organigrama general operativo conjunto con el poder judicial en Francia.

A partir de aquí el congreso se centró en la ciberdelincuencia y fue DONATAS MAZEIKA, Jefe del departamento de investigación cibercriminal en Lituania, el que detalló las formas de actuación de este departamento, concretamente en su país y la interconexión de éste con Europol. Con el mismo hilo, THAMAR VLAADEREEN Jefa de la unidad del crimen tecnológico en Holanda, expuso las formas de actuación de este departamento en su país y los lazos de éste con Europol.

A partir de aquí trataron del *modus operandi* de las diferentes unidades policiales: Primero en España, el Teniente Coronel Jefe de la unidad operativa de inteligencia criminal (UTPJ) de la Guardia Civil,JOSÉ DURÁN explicó el funcionamiento práctico en España en el caso de cualquier delito tecnológico y los procedimientos enlazados con el poder judicial; En segundo lugar, GUNNAR WEIMANN, Coordinador jefe del Centro Antiterrorista de Europol[198], comentó su funcionamiento y sus líneas de coordinación estratégica, detallando las estrategias de marketing que están utilizando las diferentes organizaciones terroristas.

Siguió DANIEL PEARCE, Jefe del programa de lucha antiterrorista en el Reino Unido, que informó acerca de la situación en su país tras los recientes ataques, refiriéndose a situaciones concretas y medios disponibles, necesarios y utilizados para poder evitar este tipo de ataques. En esta misma línea DAMIEN TRAVELETTI, oficial jefe de la policía suiza de enlace con Europol, detalló el funcionamiento en

[198] Vid. https://www.europol.europa.eu/

Suiza como país fuera de la UE y sus relaciones, estrategias, etc.

Par finalizar centrando la charla en el asunto terrorista, FRANCISCO JOSÉ VÁZQUEZ, Comandante de la Unidad de Inteligencia Antiterrorista de la Guardia Civil, explicó la operativa, medios, organización, enlace con el poder judicial y actuaciones de esta unidad en España.También expuso su experiencia en la lucha contra ETA, que les ha permitido actuar con mayor efectividad e inteligencia en la actualidad.

Una vez finalizadas las ponencias se realizaron las preguntas oportunas a los ponentes y se facilitaron mútuamente direcciones de contacto para posibles consultas e intercambio de información entre ponentes y asistentes para en el futuro, trabajar con una mayor eficacia y probabilidad de éxito, entre todos los países asistentes. El congreso fue de gran utilidad a nivel formativo, contactos y favoreció futuras colaboraciones entre países.

II.6.5.- Análisis retrospectivode los atentados NY 11 de septiembre

JOSÉ. M. BLANCO exdirector del Centro de Análisis y Prospectiva de la Guardia Civil (CAP) analiza el simbolismo que tienen algunas fechas en para las acciones del terrorismo yihadista [199].

Con ocasión del aniversario del 11S de 2001 (comenta sobre el artículo de LUIS DE LA CORTE, de ABC), aparece un debate sobre si el motivo se debe al choque de civilizaciones o a la política internacional de EE.UU., aunque la realidad es que el odio hacia Estados Unidos sigue ahí después de tantos años.

En opinión de BLANCO, el escritor PETER BERGEN, de CNN, autor de “Manhunt”, es uno de los mejores autores de libros sobre Al Qaeda y BIN LADEN, y cataloga su libro como un manual de análisis de inteligencia en sí mismo. También es de interés completar esta visión con la inversa, la que nos proporcionan

[199] BLANCO NAVARRO, J. M. (2016) Exdirector del centro de Analisis y Prospectiva de la Guardia Civil (CAP). Foro para la paz en el mediterraneo, recuperado de: https://www.uma.es/foroparalapazenelmediterraneo/?p=5741

testimonios desde el entorno de BIN LADEN en el libro "*The Exile: The Flight of Osama Bin Laden*"

BLANCO (2016) habla del comentario de BRUCE HOFFMAN, director del centro sobre seguridad de la Universidad de Georgetown, sobre estado del terrorismo en un artículo disponible en la web[200]. El experto opina que Al Qaeda no ha desaparecido sino que está esperando el desmembramiento del estado Islámico para actuar.

En definitiva, 16 años después mucho ha cambiado, pero poco ha cambiado: el fenómeno terrorista muta, evoluciona, se adaptay se perpetúa. Quedan muchos años de lucha, que no de guerra, puesto que no se trata únicamente de una cuestión militar (afecta a todos los ámbitos: político, social, económico, tecnológico, legal...; y que precisa la involucración de todos los sectores y de los ciudadanos); ni es contra un enemigo concreto (grupo, individuos) sino contra un movimiento; ni se acaba con un tratado o fumando la pipa de la paz.

BLANCO (2011) reconoce que ésto no es óbice para ser críticos con la forma en que Occidente ha fallado a sus propios valores en estos años (torturas, víctimas colaterales, prisioneros sin juicio, prisiones secretas, métodos avanzados de interrogatorio, mentiras y una invocación a la democracia que no se corresponde con la acción que se desarrolla en relaciones internacionales...). También revisa el documento que escribió para el IEEE en 2011, con ocasión del 10º aniversario de los ataques y dice que gran parte mantiene vigencia. Comenta que la solución pasa sin duda por la firmeza, la unidad, la resiliencia (pero de verdad, holística, no sólo de palabra) y la acción inteligente[201]. En el conocimiento y la inteligencia está la clave. Y en ocasiones, en dotar de los recursos necesarios a las herramientas ya existentes y que se muestran efectivas.

En definitiva, Al Qaeda no ha muerto; desde muchos ámbitos se alerta sobre la amenaza que puede seguir suponiendo, debido entre otras cosas al

[200] Vid: <www.prensaobjetiva.com>

[201] BLANCO NAVARRO, J. M. (7 de septiembre de 2011). Seguridad e inteligencia 10 años después del 11-S. Documento Marco del Instituto Español de Estudios Estratégicos (IEEE). Recuperado de: http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM09-2011SeguridadInteligencia.pdf

declive del DAESH, a la pujanza de sus franquicias en Siria y Yemen especialmente (y mantenimiento en el Magreb y Somalia), su histórica capacidad de resiliencia y adaptación, su deseo de seguir innovando y desarrollando ataques de alto impacto, la emergencia de HAMZA BIN LADEN, que puede cubrir la falta de carisma de AL ZAWAHIRI, etc.

CAPÍTULO III

RESPUESTA LEGISLATIVA ESPAÑOLA

El ciberespacio es un espacio virtual de reciente aparición, que crece exponencialmente. Es un ámbito de libertad de intercambios globales de información, con innumerables aspectos positivos, pero que así mismo puede ser utilizado para la realización de acciones delictivas y actos terroristas. Los estados trabajan para controlarlo y pese a un acelerado proceso de modernización del aparato de justicia e intento de actualización de las leyes, los delincuentes en numerosas ocasiones lograrán evadirse de la autoridad.

Todos estos cambios en el mundo, la nueva era de la comunicación, los nuevos campos de batalla, el ciberespacio es una realidad, un amplio espacio, o herramienta delictiva del cual se aprovechan los delincuentes y en el caso que nos interesa en este trabajo, los grupos terroristas están adaptados a la perfección, desenvolviéndose y utilizando este medio para llevar a cabo sus pretensiones.

"Internet era una esperanza; nos la han robado" e "Internet es un sueño para los usuarios y una pesadilla para los prácticos del Derecho"[202].

Los Estados de todo el mundo se han movilizado para contrarrestarlos, buscando la seguridad de sus habitantes. Esto les obliga a llevar a cabo nuevos planes en materia de seguridad y han tenido que actualizar sus códigos Penales para de esta forma poder abarcar con todos estos nuevos delitos que han

[202] LÓPEZ ZAMORA, P. (2006). El ciberespacio y su ordenación, Capítulo 2: Regulando el ciberespacio, Difusión jurídica y temas de actualidad, p. 95, recuperado de: http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

aparecido tanto en método como en forma. En el caso de España su Código penal ha sufrido una reciente actualización a principios del 2015, en lo referente a la materia antiterrorista:

- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP.
- Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP, en materia de delitos de terrorismo.

III.1.- MODIFICACIÓN CP (2015)

III.1.1.- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP

Es la UE la primera en el año 2002 en modificar y ampliar los delitos de terrorismo, en la decisión marco del consejo de 13 de Junio del 2002 sobre la lucha contra el terrorismo, cuando se definen en sentido amplio los delitos contra el terrorismo y se amplían estos, no solo el que los comete sino el que induce o está tentado a realizarlos, concretamente en el artículo 4. Inducción, complicidad y tentativa.

"*For the definition of terrorism, we choose the one contained in the Council Framework Decision of June 13th, 2002 on combating terrorism. The mere threat of committing such an offense should be considered a terrorist act*"[203]

En estudio individualizado y resumido de las modificaciones realizadas en la Ley Orgánica 10/1995 CP, podemos consultar todos estos cambios legislativos en la Ley[204] y en el cuadro comparativo[205] del Ilustre Colegio Oficial de Abogados

[203] MARCOS MARTÍN, T (2017), Radicalism and terrorist in the 21st century, Legal Instruments and Specific Actions in the EU's Fight against Terrorism, página 248.

[204] Vid. Código penal, Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, (31/03/1995). *Boletín Oficial del Estado (BOE)*, nº 77.

[205] Vid. Anexo IV.Ilustre Colegio de Abogados de Madrid. Cuadro comparativo Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Recuperado de tabla comparativa: http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

de Madrid, donde se comparan dichos cambios.

III.1.2.- Ley Orgánica 2/2015, de 30 de marzo por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP en materia de delitos de terrorismo

A continuación se describen los artículos de la Ley que centran principalmente la base legal delpresente estudio: arts. 571 a 580.

«CAPÍTULO VII: De las organizaciones y grupos terroristas y de los delitos de terrorismo.

Sección 1ª. De las organizaciones y grupos terroristas.

Artículo 571. A los efectos de este Código 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 ter, tengan por finalidad o por objeto la comisión de alguno de los delitos tipificados en la sección siguiente.

Artículo 572. 1. Quienes promovieran, constituyeran, organizaran o dirigieran una organización o grupo terrorista serán castigados con las penas de prisión de ocho a catorce años e inhabilitación especial para empleo o cargo público por tiempo de ocho a quince años. 2. Quienes participaran actívamente en la organización o grupo, o formaran parte de ellos, serán castigados con las penas de prisión de seis a doce años e inhabilitación especial para empleo o cargo público por tiempo de seis a catorce años.

Sección 2ª. De los delitos de terrorismo.

Artículo 573. 1. Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves,

buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades: 1ª 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. 2ª Alterar gravemente la paz pública. 3ª Desestabilizar gravemente el funcionamiento de una organización internacional. 4ª Provocar un estado de terror en la población o en una parte de ella. 2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior. 3. Asímismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo.

Artículo 573 bis. 1. Los delitos de terrorismo a los que se refiere el apartado 1 del artículo anterior serán castigados con las siguientes penas: 1ª Con la de prisión por el tiempo máximo previsto en este Código si se causara la muerte de una persona. 2ª Con la de prisión de veinte a veinticinco años cuando, en los casos de secuestro o detención ilegal, no se dé razón del paradero de la persona. 3ª Con la de prisión de quince a veinte años si se causara un aborto del artículo 144, se produjeran lesiones de las tipificadas en los artículos 149, 150, 157 o 158, el secuestro de una persona, o estragos o incendio de los previstos respectívamente en los artículos 346 y 351. 4ª Con la de prisión de diez a quince años si se causara cualquier otra lesión, o se detuviera ilegalmente, amenazara o coaccionara a una persona.

5ª Y con la pena prevista para el delito cometido en su mitad superior, pudiéndose llegar a la superior en grado, cuando se tratase de cualquier otro de los delitos a que se refiere el apartado 1 del artículo anterior. 2. Las penas se impondrán en su mitad superior si los hechos se cometieran contra las personas mencionadas en el apartado 3 del artículo 550 o contra miembros de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas o contra empleados públicos que presten servicio en instituciones penitenciarias. 3. Los delitos de terrorismo a los que se refiere el apartado 2 del artículo anterior se castigarán con la pena superior en grado a la respectívamente prevista en los correspondientes artículos. 4. El delito de desórdenes públicos previsto en el artículo 557 bis, así como los

delitos de rebelión y sedición, cuando se cometan por una organización o grupo terrorista o individualmente pero amparados en ellos, se castigarán con la pena superior en grado a las previstas para tales delitos.

Artículo 574. 1. El depósito de armas o municiones, la tenencia o depósito de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o de sus componentes, así como su fabricación, tráfico, transporte o suministro de cualquier forma y la mera colocación o empleo de tales sustancias o de los medios o artificios adecuados, serán castigados con la pena de prisión de ocho a quince años cuando los hechos se cometan con cualquiera de las finalidades expresadas en el apartado 1 del artículo 573. 2. Se impondrá la pena de diez a veinte años de prisión cuando se trate de armas, sustancias o aparatos nucleares, radiológicos, químicos o biológicos, o cualesquiera otros de similar potencia destructiva. 3. Serán también castigados con la pena de diez a veinte años de prisión quienes, con las mismas finalidades indicadas en el apartado 1, desarrollen armas químicas o biológicas, o se apoderen, posean, transporten, faciliten a otros o manipulen materiales nucleares, elementos radioactivos o materiales o equipos productores de radiaciones ionizantes.

Artículo 575. 1. Será castigado con la pena de prisión de dos a cinco años quien, con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo, reciba adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o específicamente destinados a facilitar la comisión de alguna de tales infracciones.

2. Con la misma pena se castigará a quien, con la misma finalidad de capacitarse para cometer alguno de los delitos tipificados en este Capítulo, lleve a cabo por sí mismo cualquiera de las actividades previstas en el apartado anterior. Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera

de ellos o en sus fines. Los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español. Asímismo se entenderá que comete este delito quien, con la misma finalidad, 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.

3. La misma pena se impondrá a quien, para ese mismo fin, o para colaborar con una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo, se traslade o establezca en un territorio extranjero controlado por un grupo u organización terrorista.

Artículo 576. 1. Será castigado con la pena de prisión de cinco a diez años y multa del triple al quíntuplo de su valor el que, por cualquier medio, directa o indirectamente, recabe, adquiera, posea, utilice, convierta, transmita o realice cualquier otra actividad con bienes o valores de cualquier clase 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. 2. Si los bienes o valores se pusieran efectivamente a disposición del responsable del delito de terrorismo, se podrá imponer la pena superior en grado. Si llegaran a ser empleados para la ejecución de actos terroristas concretos, el hecho se castigará como coautoría o complicidad, según los casos. 3. En el caso de que la conducta a que se refiere el apartado 1 se hubiera llevado a cabo atentando contra el patrimonio, cometiendo extorsión, falsedad documental o mediante la comisión de cualquier otro delito, éstos se castigarán con la pena superior en grado a la que les corresponda, sin perjuicio de imponer además la que proceda conforme a los apartados anteriores. 4. El que estando específicamente sujeto por la ley a colaborar con la autoridad en la prevención de las actividades de financiación del terrorismo dé lugar, por imprudencia grave en el cumplimiento de dichas obligaciones, a que no sea detectada o impedida cualquiera de las conductas descritas en el apartado 1 será castigado con la pena inferior en uno o dos grados a la prevista en él. 5. Cuando, de acuerdo con lo establecido en el artículo 31 bis, una persona jurídica sea responsable de los delitos tipificados en este artículo se le impondrán las siguientes penas: a) Multa de dos a cinco años si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco

años. b) Multa de uno a tres años si el delito cometido por la persona física tiene prevista una pena de más de dos años de privación de libertad no incluída en la letra anterior. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas previstas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 577. 1. Será castigado con las penas de prisión de cinco a diez años y multa de dieciocho a veinticuatro meses el que lleve a cabo, recabe o facilite cualquier acto de colaboración con las actividades o las finalidades de una organización, grupo o elemento terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo. En particular son actos de colaboración la información o vigilancia de personas, bienes o instalaciones, la construcción, acondicionamiento, cesión o utilización de alojamientos o depósitos, la ocultación, acogimiento o traslado de personas, la organización de prácticas de entrenamiento o la asistencia a ellas, la prestación de servicios tecnológicos, y cualquier otra forma equivalente de cooperación o ayuda a las actividades de las organizaciones o grupos terroristas, grupos o personas a que se refiere el párrafo anterior.

Cuando la información o vigilancia de personas mencionada en el párrafo anterior ponga en peligro la vida, la integridad física, la libertad o el patrimonio de las mismas se impondrá la pena prevista en este apartado en su mitad superior. Si se produjera la lesión de cualquiera de estos bienes jurídicos se castigará el hecho como coautoría o complicidad, según los casos. 2. Las penas previstas en el apartado anterior se impondrán a quienes lleven a cabo cualquier actividad de captación, adoctrinamiento o adiestramiento, que esté dirigida o que, por su contenido, resulte idónea para incitar a incorporarse a una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo. Asimismo se impondrán estas penas a los que faciliten adiestramiento o instrucción sobre la fabricación o uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre métodos o técnicas especialmente adecuados para la comisión de alguno de los delitos del artículo 573, con la intención o conocimiento de que van a ser utilizados para ello. Las penas se impondrán en su mitad superior, pudiéndose llegar a la superior en grado, cuando los actos previstos en este apartado se hubieran dirigido a menores de edad o personas con discapacidad necesitadas de especial protección o a mujeres

víctimas de trata con el fin de convertirlas en cónyuges, compañeras o esclavas sexuales de los autores del delito, sin perjuicio de imponer las que además procedan por los delitos contra la libertad sexual cometidos. 3. Si la colaboración con las actividades o las finalidades de una organización o grupo terrorista, o en la comisión de cualquiera de los delitos comprendidos en este Capítulo, se hubiera producido por imprudencia grave se impondrá la pena de prisión de seis a dieciocho meses y multa de seis a doce meses.

Artículo 578. 1. El enaltecimiento o la justificación públicos de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares, se castigará con la pena de prisión de uno a tres años y multa de doce a dieciocho meses. El juez también podrá acordar en la sentencia, durante el período de tiempo que él mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57. 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. 3. Cuando los hechos, a la vista de sus circunstancias, resulten idóneos para alterar gravemente la paz pública o crear un grave sentimiento de inseguridad o temor a la sociedad o parte de ella se impondrá la pena en su mitad superior, que podrá elevarse hasta la superior en grado. 4. El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos o cualquier otro soporte por medio del que se hubiera cometido el delito. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación se acordará la retirada de los contenidos. Si los hechos se hubieran cometido a través de servicios o contenidos accesibles a través de internet o de servicios de comunicaciones electrónicas, el juez o tribunal podrá ordenar la retirada de los contenidos o servicios ilícitos. Subsidiariamente, 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 siempre que concurra alguno de los siguientes supuestos: a) Cuando la medida resulte proporcionada a la gravedad de los hechos y a la relevancia de la información y necesaria para evitar su difusión. b) Cuando se difundan exclusiva o preponderantemente los contenidos a los que se refieren los apartados anteriores. 5. Las medidas previstas en el apartado anterior podrán también ser acordadas por el juez instructor con carácter cautelar durante la instrucción de la causa.

Artículo 579. 1. Será castigado con la pena inferior en uno o dos grados a la prevista para el delito de que se trate el que, por cualquier medio, difunda públicamente mensajes o consignas que tengan como finalidad o que, por su contenido, sean idóneos para incitar a otros a la comisión de alguno de los delitos de este Capítulo. 2. La misma pena se impondrá al que, públicamente o ante una concurrencia de personas, incite a otros a la comisión de alguno de los delitos de este Capítulo, así como a quien solicite a otra persona que los cometa. 3. Los demás actos de provocación, conspiración y proposición para cometer alguno de los delitos regulados en este Capítulo se castigarán también con la pena inferior en uno o dos grados a la que corresponda respectivamente a los hechos previstos en este Capítulo. 4. En los casos previstos en este precepto, los jueces o tribunales podrán adoptar las medidas establecidas en los apartados 4 y 5 del artículo anterior.

Artículo 579 bis. 1. El responsable de los delitos previstos en este Capítulo, sin perjuicio de las penas que correspondan con arreglo a los artículos precedentes, será también castigado, atendiendo proporcionalmente a la gravedad del delito, el número de los cometidos y a las circunstancias que concurran en el delincuente, con las penas de inhabilitación absoluta, inhabilitación especial para profesión u oficio educativos, en los ámbitos docente, deportivo y de tiempo libre, por un tiempo superior entre seis y veinte años al de la duración de la pena de privación de libertad impuesta en su caso en la sentencia. 2. Al condenado a pena grave privativa de libertad por uno o más delitos comprendidos en este Capítulo se le impondrá además la medida de libertad vigilada de cinco a diez años, y de uno a cinco años si la pena privativa de libertad fuera menos grave. No obstante lo anterior, cuando se trate de un solo delito que no sea grave y su autor hubiere delinquido por primera vez, el tribunal podrá imponer o no la medida

de libertad vigilada, en atención a su menor peligrosidad. 3. En los delitos previstos en este Capítulo, los jueces y tribunales, razonándolo en sentencia, podrán imponer la pena inferior en uno o dos grados a la señalada para el delito de que se trate, cuando el sujeto haya abandonado voluntariamente sus actividades delictivas, se presente a las autoridades confesando los hechos en que haya participado y colabore activamente con éstas para impedir la producción del delito, o coadyuve eficazmente a la obtención de pruebas decisivas para la identificación o captura de otros responsables o para impedir la actuación o el desarrollo de organizaciones, grupos u otros elementos terroristas a los que haya pertenecido o con los que haya colaborado. 4. Los jueces y tribunales, motivadamente, atendiendo a las circunstancias concretas, podrán imponer también la pena inferior en uno o dos grados a la señalada en este Capítulo para el delito de que se trate, cuando el hecho sea objetivamente de menor gravedad, atendidos el medio empleado o el resultado producido.

Artículo 580. En todos los delitos de terrorismo, la condena de un juez o tribunal extranjero será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia».

Disposición final primera. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Se modifica el apartado 4 e) 2º del artículo 23 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que queda redactado como sigue: «2º el procedimiento se dirija contra un extranjero que resida habitualmente o se encuentre en España o, sin reunir esos requisitos, colabore con un español, o con un extranjero que resida o se encuentre en España, para la comisión de un delito de terrorismo»[206].

III.2.- DELITOS ESPECÍFICOS

Para la tipificación de los delitos de terrorismo informático empezaremos haciendo un recorrido por los conceptos inherentes a su ejecución.

[206] Vid. Código penal, Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, (31/03/1995). *Boletín Oficial del Estado (BOE)*, nº 77.

El Grupo de trabajo C-24: Derecho & cibercrimen (2009), empieza definiendo el **cibercrimen** como un concepto que abarca los delitos económicos, el fraude informático, el robo, la falsificación, el*computer hacking*, el espionaje informático, el sabotaje y extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad y el crimen organizado (RODRÍGUEZ BERNAL, 2007: 9)[207].

Para ROVIRA DEL CANTO(2011), el **ciberdelito** se presenta no sólo como manifestación global y genérica de la criminalidad informática originada por el riesgo propio del uso y utilización de la informática, la telemática y de la información en la actual sociedad, y por tanto como categoría funcional o criminológica, sino además como concepto para referirnos a un conjunto de figuras normativas de tipos delictivos con entidad y sustantividad propia, y que conformarían el núcleo de lo que ha venido formulando como Derecho Penal Global del Riesgo Informático y de la Información, en donde el delito informático *strictu sensu* viene configurado como un delito pluriofensivo, en el que hay que tener siempre concurrente la protección de los nuevos intereses derivados de la sociedad global del riesgo informático y de la información (la información en sí misma, los datos informáticos, que son la representación de aquélla, y la fiabilidad y seguridad colectiva en los medios y sistemas de tratamiento y transferencia de la información).

Otra categorización de estos delitos la presenta LÓPEZ GARCÍA[208], que clasifica los delitos cometidos y los sujetos que los ejecutan.

[207] GRUPO DE TRABAJO C-24. (2009). Derecho & cibercrimen. Internet: Un espacio para el cibercrimen y el ciberterrorismo. Recuperado de:http://www.cibersociedad.net/congres2009/es/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610

[208] LÓPEZ GARCÍA, L. Y. (2016). Proyecto estratégico de prevención de la cibercriminalidad para México en la globalización (una mirada desde el extranjero). Facultad de Derecho y Ciencias Sociales - División de estudios de postgrado. México.

CLASE DE DELITO	SUJETOS
Delitos patrimoniales contra bancos y entidades financieras	Empleados, en especial cajeros o personal del área de sistemas, ex empleados.
Delitos de acceso ilegítimo o delito de daños menores	Hackers, phreakers, usuarios descontentos
Daño o sabotaje informático	Empleados de la empresa, o espías profesionales o industriales
Violaciones a la privacidad, tratamiento ilícito de datos personales	Investigadores privados, empresas de marketing,agencias de informes crediticios y solvencia patrimonial
Violaciones a la propiedad intelectual del software y bancos de daños, con informes o compilaciones de datos	Piratas informáticos, o también usuarios ("la copia amigable"), empresas que realizan competencia "parasitaria".

Ilustración 33: *Clases de delitos y sujetos. Delitos informáticos*[209].

Como podemos observar en la ilustración 33 la diferencia radica en que estos delincuentes se valen del ciberespacio para realizar sus actividades delictivas. En cambio, el ciberterrorismo va más allá de la ciberdelincuencia, por mucho que algunos consideren que ambos son una misma cosa. Indudablemente tienen cierta vinculación, porque en muchas ocasiones los ciberterroristas desempeñan actividades delictivas en la red, pero las causas que las motivan y los beneficios que esperan unos y otros son diferentes. Por tanto "El ciberterrorismo es la convergencia del ciberespacio y el terrorismo, es decir, la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines político-religiosos". Por tanto, viene a ser la evolución que resulta de cambiar las armas, las bombas y los misiles por una computadora para planificar y ejecutar unos ataques que

[209] Ibídem.

produzcan los mayores daños posibles a la población civil. Esto implica una gran diferencia respecto al cibercrimen: el ciberterrorismo busca originar el mayor daño posible por razones político-religiosas mientras que las acciones del cibercrimen están dirigidas a conseguir un beneficio principalmente económico.

Estas definiciones de **ciberterrorismo** tienen su raíz en la definición de las acciones terroristas CP español[210]; que en su Artículo573 define estas acciones así:

1. Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1ª 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.
2ª Alterar gravemente la paz pública.
3ª Desestabilizar gravemente el funcionamiento de una organización internacional.
4ª Provocar un estado de terror en la población o en una parte de ella.

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo.

[210] Vid. Ley Orgánica 10/1995, de 23 de noviembre, del Código penal, (1995).

El análisis del art. 573 por parte de PONTE (2015) en su texto "La reforma de los delitos de terrorismo mediante la Ley Orgánica 2/2015", resume los delitos de terrorismo como sigue:

*Es **delito de terrorismo** la comisión de cualquier delito con la siguiente finalidad:*

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.
2. Obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.
3. Alterar gravemente la paz pública.
4. Desestabilizar gravemente el funcionamiento de una organización internacional.
5. Provocar un estado de terror en la población o en una parte de ella.
6. Se destaca expresamente la comisión de delitos informáticos (art. 197 bis y 197 ter y 264 a 264 quater) con la misma finalidad.

En el mismo documento, PONTE (2015) presenta un análisis de las principales novedades en cuanto a regulación penal que reposan en el código penal español en sus artículos 571 al 580 en relación a su nueva redacción.

1. Se amplía el catálogo de las "finalidades" terroristas, comprendiendo como tales no sólo subvertir el orden constitucional, sino además suprimir o desestabilizar el funcionamiento de instituciones políticas o estructuras económicas o sociales del Estado; obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo; desestabilizar el funcionamiento de una organización internacional o provocar estado de terror en población.

2. Se introduce expresamente la configuración de los delitos informáticos como delitos de terrorismo cuando se cometan con las finalidades terroristas descritas anteriormente.

3. Se tipifica el delito de desórdenes públicos, el delito de sedición y el de rebelión como delitos de terrorismo si se cometen por organización o

grupo terrorista o por persona o personas que los cometan individualmente, pero amparados por organización o grupo terrorista.

4. Se prevé como delito de terrorismo el adoctrinamiento o adiestramiento en técnicas militares, de combate, de preparación o de desarrollo de armas, explosivos, armas químicas o biológicas, o sustancias inflamables, incendiarias, explosivas, etc. Esta conducta se castiga bien al recibir adiestramiento de terceros o bien "capacitándose" a sí mismo, es decir, el autodidacta.

5. Se tipifica como delito el que, con esta finalidad de adiestrarse, tenga en su poder documentos, archivos, o acceda de forma habitual a servicios de comunicación vía internet o electrónica cuyos contenidos sean idóneos para incitar a la incorporación a organizaciones o grupos terroristas o a colaborar con cualquiera de ellos.

6. Se tipifica como delito de terrorismo el desplazamiento o establecimiento a un territorio extranjero controlado por un grupo u organización terrorista para recibir adiestramiento o para colaborar con ellos

7. En cuanto al delito de colaboración, se amplía el catálogo de conductas sancionadas. Además, será colaboración la ayuda tanto a una organización o grupo terrorista como a grupos o a individuos cuyas acciones tengan finalidad terrorista.

8. En relación a los delitos de enaltecimiento o actos de humillación, descrédito o menosprecio a las víctimas del terrorismo, cabe la adopción judicial de medidas cautelares en el caso de que dichos delitos se cometan mediante servicios o contenidos accesible a través de internet o de servicios de comunicaciones electrónicas. Se podrá ordenar la retirada de los contenidos, la supresión de los enlaces y la prohibición de acceso a dichos contenidos ilícitos.

La reforma, es un gran avance, por tanto, en relación a la prevención del impulso del terrorismo yihadista a través de redes sociales, comunicaciones electrónicas o creación de páginas web o foros, penando tanto la difusión de ideas

incitadoras como el adiestramiento en técnicas para la comisión de cualquier delito de terrorismo. También supone un importante apoyo legislativo la penalización de los desplazamientos a territorios controlados por organizaciones o grupos terroristas, para recibir adiestramiento o adoctrinamiento, tipificándolos como delito.

Entre las motivaciones que tienen las acciones de ciberterrorismo el FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: *Money, Ideology, Compromise* y *Ego* (Dinero, Ideología, Compromiso y Autorrealización personal) (GÓMEZ VIEITES, 2014). En general, podemos considerar la siguiente tipología de motivaciones de los atacantes:

- Consideraciones económicas: llevar a cabo operaciones fraudulentas; robo de información confidencial que posteriormente es vendida a terceros; extorsiones (si no se paga un determinado "rescate" se elimina información o se daña de forma irreparable un sistema que haya sido comprometido); intentos de manipulación de las cotizaciones de valores bursátiles; etcétera.

- Diversión: algunos usuarios de Internet realizan estos ataques como una forma de pasar el rato delante de su ordenador.

- Ideología: ataques realizados contra determinadas organizaciones, empresas y Websites gubernamentales, con un contenido claramente político.

- Autorrealización.

- Búsqueda de reconocimiento social y de un cierto *estatus* dentro de una comunidad de usuarios.

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas; deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido). Estos tres

factores constituyen lo que podríamos denominar como el "Triángulo de la Intrusión", concepto que se presenta de forma gráfica en la ilustración 34:

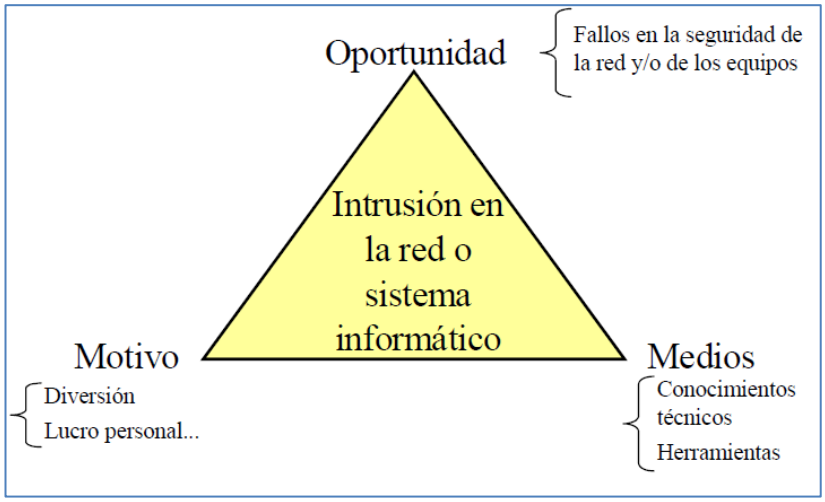


Ilustración 34: *La lucha contra el ciberterrorismo y los ataques informáticos. Memorias X Reunión Española Sobre Criptología y Seguridad de la Información*[211]*.*

CANO (2008), analiza los aspectos criminológicos y legales del terrorismo desde el estudio del terrorismo islamista y el uso de internet como un binomio en la época actual. "En una era marcada por la globalización de las comunicaciones y el uso de la red global de Internet por miles de millones de usuarios en todo el planeta, hace que el uso de este medio de comunicación pueda producirse con objetivos radicalmente dispares. En el concreto caso del terrorismo islamista, el uso que viene haciéndose de Internet por esta denominada "ideología del odio" representada por *Al Qaeda* puede sintetizarse en los siguientes aspectos:

- Como instrumento para llevar a cabo o amenazar con la ejecución de ataques contra las redes computarizadas que proveen servicios públicos, tales como los sistemas de control de energía, redes de ferrocarril, aeropuertos, sistemas financieros, de seguridad, etc., es lo que se conoce como "ciberterrorismo";
- Como medio para intercambiar noticias y mensajes electrónicos encriptados que contienen importante información acerca de la planificación de atentados terroristas;

[211] GÓMEZ VIEITES, Á. (1 de agosto de 2014). La lucha contra el ciberterrorismo y los ataques informáticos. Ponencia X Reunión española sobre criptología y seguridad de la información, pp. 251-261. Recuperado de: http://www.edisa.com/wp-content/uploads/2014/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

- Como foro de propaganda del terrorismo islamista, ensalzando y justificando la *yihad* contra los infieles mediante la distribución en la red de vídeos que contienen ataques terroristas, asesinatos de rehenes, discursos de imanes radicales o miembros destacados de Al Qaeda, así como vídeos de despedida de los futuros mártires de *Allah*;
- Como medio para recaudar fondos, por ejemplo, a través de donativos administrados por sociedades benéficas, asociaciones no gubernamentales u organizaciones islamistas radicales que disponen de "sedes virtuales" en Internet;
- Como "oficina de reclutamiento" para los futuros terroristas islamistas, utilizando para ello los innumerables foros de Chat que son visitados por miles de individuos receptivos a la ideología yihadista;
- Como "campo de entrenamiento virtual" para los futuros *mujahedines*, los cuales a través de la red pueden adquirir los conocimientos necesarios no sólo para realizar actividades de insurgencia y terrorismo, sino también para construir artefactos explosivos con los que llevar a cabo sus acciones terroristas;
- Como plataforma de adoctrinamiento y radicalización *yihadista* de cientos de miles de individuos musulmanes repartidos por todo el mundo que, por diversas razones, sienten la necesidad de defender al Islam del yugo representado por Occidente"[212].

Uno de los detonantes de las acciones descritas en párrafos anteriores en gran parte se debe al hecho de que el enfado de los jóvenes musulmanes es susceptible de amplificarse gracias a la tecnología del siglo XXI. Efectivamente, mientras que en el pasado estos jóvenes alienados de sus sociedades "hervían a fuego lento" inmersos en un relativo aislamiento, incapaces de conectar o comunicarse con otros sujetos que compartían sus problemas, hoy en día Internet ha cambiado radicalmente esta situación. Es indudable que la red global de Internet ha supuesto un elemento crucial para la expansión de lo que se conoce ya como "generación yihad", haciendo posible que sujetos separados por miles de

[212] CANO PAÑOS, M. Á. (2008). Internet y terrorismo islamista. Aspectos criminológicos y legales. *EGUZKILORE Cuaderno del Instituto Vasco de Criminología* nº 22, pp. 67-88. Recuperado de: http://www.ehu.eus/documents/1736829/2176658/03+Cano.indd.pdf

kilómetros y asentados en sociedades distintas puedan comunicarse entre ellos e intercambiar tanto experiencias como información, la cual en no pocas ocasiones se debe a la proliferación y sofisticación de la propaganda yihadista a través de red (CANO PAÑOS, 2008).

Estas acciones han sido reconocidas en el Código Penal español que en su capítulo "del descubrimiento y revelación de secretos" y de "los daños":

Artículo 197:

(…) 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. (….).

Artículo 197 bis:

1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, (….).

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de

información, incluidas las emisiones electromagnéticas de los mismos, (…..).

Artículo 197 ter:

Será castigado con una pena de prisión (…) el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a. Un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b. Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 264:

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1ª Se hubiese cometido en el marco de una organización criminal.

2ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un

Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 bis:

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizará o interrumpiera el funcionamiento de un sistema informático ajeno:

a. Realizando alguna de las conductas a que se refiere el artículo anterior;
b. Introduciendo o transmitiendo datos; o
c. Destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado

2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

En el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo[213].

III.2.1.- Captación y entrenamiento

La Decisión Marco de 2008 en la lucha de la Unión Europea contra el terrorismo[214], establece la definición de los conceptos de captación y entrenamiento:

CAPTACIÓN DE TERRORISTAS: aquella petición a otra persona para que cometa delitos terroristas.Su objetivo suele centrarse en personas jóvenes y vulnerables debido a su conducta anti-social o que estén desorientados ofreciéndole la oportunidad de poder vengarse de las injusticias que ha cometido la vida con él o ella a través del yihadismo.

[213] Vid.Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[214] MARTÍNEZ DE SALAS Y SÁNCHEZ - Abogados. (2016). La captación terrorista. Recuperado de http://www.martinezdesalasysanchez.com/noticias/2016/01/16/la-captacion-terrorista.html

El *modus operandi* es muy sencillo. Los grupos terroristas usan las redes sociales a través de la creación de cuentas para atraer la curiosidad de los jóvenes, conteniendo propaganda, videos y gráficos manipulados. Cuando consiguen atraer su atención, hacen un análisis de su personalidad recopilando toda la información de la que pueden disponer (edad, educación, formación, familia…) y sobre este perfil, se le anima a la creación de un grupo de conversaciones con otros jóvenes, siendo esta gente perteneciente al grupo terrorista con la intención de hacer que se una al grupo terrorista. Tras esto, se le ofrece tener contacto en persona, donde usan personas con carisma y buenas habilidades en relaciones sociales. Por último, buscan la forma de convencerles de que viaje a uno de sus destinos.

Según los datos policiales, en 2014 más de 70 residentes en España estaban combatiendo en el Estado Islámico. Se detuvo a 41 yihadistas en 12 operaciones con el objeto de desarticular estas células. En Europa se ha atraído a más de 3.000 europeos, siendo Rusia y Francia los países con más combatientes. Durante el 2015, los datos se han cuadriplicado, siendo 90 yihadistas detenidos y otros 300 investigados.

La captación es mucho más complicada en aquellas comunidades dónde haya menos inmigración marroquí y argelina, ya que, más de la mitad de los detenidos o que están al frente de las operaciones yihadistas no son españoles de origen. Por tanto, Ceuta y Melilla representan el 75% total de la procedencia de los arrestados en España seguida de Barcelona que representa un significativo 5%.

La influencia de internet es tal que traspasa fronteras. Un informe del instituto de inteligencia Soufan Group, menciona a Latinoamérica como un área de reclutamiento y, principalmente, de entrenamiento de futuros terroristas. Los tentáculos del Estado Islámico ya han llegado a la región, aprovechando las rutas del narcoterrorismo, la permisividad de los gobiernos de algunos países, la falta de control de otros y utilizando las fronteras sin vigilancia entre diversas naciones para entrenar a los recién captados. En el afán de reclutar soldados para su causa, el Estado Islámico se “globaliza”a un ritmo imparable. Ésa es la conclusión a la que llegan expertos en antiterrorismo y seguridad e informes de inteligencia de las

agencias más prestigiosas del mundo. En este contexto, surge un escenario inusitado. Los terroristas se están expandiendo cada vez más en Latinoamérica, donde captan y entrenan a sus futuros soldados.Argentina tiene antecedentes relativamente recientes en materia de atentados terroristas, como los ocurridos durante la década de los 90 contra la sede de la mutual judía AMIA, y la Embajada de Israel (ambos en Buenos Aires)[215].

Antes de los atentados del 11-S, los islamistas que operaban en Europa llevaban a cabo sus actividades de captación, reclutamiento y radicalización abiertamente en el entorno de ciertas mezquitas. Como ejemplo de mezquitas afines al Islam radical que con el tiempo se convirtieron en centros de afiliación a la causa yihadista pueden citarse entre otras la de *Finsbury Park* en Londres, la de Al-Quds en Hamburgo o la mezquita de la M-30 en Madrid. En el caso de Londres, el clérigo radical ABU HAMZA AL-MASRI utilizó en su momento la mezquita de *Finsbury Park* para difundir entre los fieles su visión radical del Islam (CANO PAÑOS, 2008).

La Directiva de la Comisión Europea en su Artículo 6 (2015) reza: Los Estados miembros adoptarán las medidas necesarias para garantizar que la incitación a otra persona para que cometa cualquiera de los delitos enumerados en el artículo 3, constituya un delito punible cuando se cometa dolosamente.

Asimismo las reformas han considerado la evolución de diversos delitos como indica el análisis de PONTE (2015) sobre el art. 575.- ADIESTRAMIENTO se tiene como finalidad: capacitarse para la comisión de delitos de terrorismo.

Conducta tipificada:

1.- Recibir adoctrinamiento o adiestramiento.

- *Militar o de combate.*
- *Técnicas de desarrollo de armas químicas o biológicas.*
- *Técnicas de elaboración o preparación de sustancias o aparatos*

[215] NOTICIAS INTERNACIONALES. (13 de diciembre de 2015). Estado Islámico extiende sus tentáculos de captación y entrenamiento a Latinoamérica. *lainformacion.com.* Recuperado de: http://www.lainformacion.com/mundo/estado-islamico-extiende-sus-tentaculos-de-captacion-y-entrenamiento-a-latinoamerica_iR7KLTuwFzmQKffCsdPsc5/

explosivos, inflamables, incendiarios o asfixiantes.

- *Facilitar la comisión de tales infracciones.*

2.- Aprender por sí mismo cualquiera de las anteriores actividades (autodidacta).

3.- Acceder de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines.

Los hechos se entenderán cometidos en el territorio español cuando se acceda a los contenidos desde el territorio español.

4.- Adquirir o tener en su poder documentos que estén dirigidos o resulten idóneos por su contenido para incitar a la incorporación a una organización o grupo terrorista o a colaborar con ellos.

5.- Traslado o establecimiento en un territorio extranjero controlado por grupo u organización terrorista para colaborar con ellos o para cometer cualquier delito de terrorismo.

Penalidad: 2 a 5 años.La directiva de la comisión europea (COMISIÓN EUROPEA, 2015) indica: Artículo 7. Adiestramiento de terroristas. Los Estados miembros adoptarán las medidas necesarias para garantizar que la impartición de 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 cualquiera de los delitos enumerados en el artículo 3, apartado 2, letras a) a h), a sabiendas de que las enseñanzas impartidas se utilizarán para dichos fines, constituya un delito punible cuando se cometa dolosamente.

La Decisión Marco de 2008 en la lucha de la Unión Europea contra el terrorismo, establece la definición de este concepto:

Adiestramiento de terroristas: dar instrucciones sobre la fabricación o 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 delitos terroristas.

CANO, expresa que con todo, y a pesar de la importancia de las mezquitas en los procesos de reclutamiento y radicalización, muchos jóvenes musulmanes son introducidos paulatinamente en la ideología del Islam radical en pequeños grupos (por ejemplo, asociaciones de estudiantes), los cuales en principio no apoyan directamente el terrorismo. "Estos grupos a menudo están compuestos por jóvenes que han nacido y crecido en el mismo barrio, siendo amigos desde la infancia. En el caso del grupo de amigos, las discusiones en torno al Islam y la yihad se celebran frecuentemente en pisos, residencias de estudiantes o en las sedes de asociaciones islámicas, lo cual dificulta seriamente el trabajo de las fuerzas de seguridad a la hora de controlar sus actividades. De un modo más o menos espontáneo, estos grupos forman un pequeño *clúster* con el denominador común de adoptar una interpretación radical del Islam. En este entorno cercano hay que añadir en casi todos los casos la presencia y actividad de por los menos un reclutador radical, si bien en los últimos tiempos la red global de Internet puede suplir la presencia de dichos individuos. Efectivamente, hasta épocas recientes es evidente que, en ausencia de contactos con un reclutador, el joven musulmán o el grupo de amigos hubieran sufrido un progresivo aislamiento. Es posible que éstos pudieran intentar participar en la yihad contra los infieles, pero sin los conocimientos necesarios, recursos o coordinación con otras células islamistas. Hoy en día, Internet ha hecho posible que en no pocas ocasiones la presencia de un reclutador sea un elemento innecesario en el proceso de radicalización en el seno de grupos"[216].

Asimismo, los encargados de reclutar miembros para la yihad suelen acudir también a los ciber-cafés y a las salas de Chat para buscar a jóvenes que muestran una predisposición hacia el islamismo radical. Una mención especial dentro de los 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. De

[216] CANO PAÑOS, M. Á. (2008). Ob., cit.

hecho, muchos de los posteriores terroristas islamistas comenzaron su conversión hacia la rama más radical del Islam navegando por Internet, visitando las miles de páginas Web y foros de Chat adscritos al fundamentalismo islamista. En este sentido, no resulta exagerado afirmar que lo que para las organizaciones terroristas tradicionales constituía la publicación clandestina o la emisión de radio ilegal ha sido sustituido por la red global de Internet, con cientos de miles de potenciales "lectores" en todo el mundo[217] (CANO PAÑOS, 2008).

CANO cita en su obra a THEVESSEN que nos habla de internet como via de conexión, "Internet posibilita entre otras cosas la cohesión global de todos los musulmanes extremistas repartidos por todo el mundo. Para el mencionado autor, la llamada "*umma virtual*" que representa Internet permite a muchos sujetos que se sienten aislados en la sociedad en la que desarrollan sus vidas percibir una sensación de pertenencia a una comunidad de sujetos unidos por una ideología común. En el caso de los jóvenes musulmanes desilusionados y alienados que habitan en Occidente, esta identificación con una umma de carácter supranacional puede conducir a la larga a un proceso de radicalización política. En este sentido, está fuera de toda duda que sin Internet hubiera resultado imposible conseguir lo que se ha denominado globalización del terrorismo islamista"[218].

EL PROCESO DE RADICALIZACIÓN. FASES

Se entiende por radicalización islamista el complejo proceso de socialización de determinados sujetos de religión musulmana dirigido generalmente por actores islamistas[219]. Este proceso tiene fundamentalmente un

[217] RAMELSBERGER, A. (2008). Der Deutsche Dschihad, p. 196: "Para el actual Ministro del Interior alemán, Wolfgang Schäuble, Internet se ha convertido en el medio del terrorismo islamista por excelencia, señalando que "la red de Internet se presenta para los terroristas como universidad a distancia y campo de entrenamiento, bolsa de intercambio de noticias y oficina de reclutamiento".

[218] CANO PAÑOS, M. Á. (2008). Ob., cit. Thevessen (pp. 82 y ss.). Según ROY, la *umma* no está hoy en día encarnada por un territorio concreto. Por el contrario, la umma imaginaria se crea más bien de manera virtual, reuniendo a aquéllos que han roto con su entorno para no definirse más que a partir de criterios islámicos. Esta umma virtual constituye en esencia una comunidad de los creyentes al margen de toda nación, de todo territorio, incluso de todo contexto social. Este espacio imaginario es el de una comunidad religiosa en un mundo hostil o indiferente. Véase: ROY, OLIVIER (2003): El Islam mundializado. Los musulmanes en la era de la globalización (Trad. por JOSÉ RAMÓN MONREAL), Barcelona: Ediciones Bellaterra, pp. 157 y 174.

[219] Ibídem.

componente social y otro ideológico: Bajo la influencia de la ideología radical islamista, la cual es transmitida a través de diversos canales, se produce la integración del individuo que está siendo radicalizado en grupos extremistas de carácter subcultural. Llegado el caso, este proceso de radicalización puede conducir a que el sujeto radicalizado exprese su disposición a unirse a organizaciones terroristas con el fin de llevar a cabo la yihad contra los infieles. Para el Servicio holandés de Seguridad e Información (AIVD), el "reclutamiento para la yihad" puede ser entendido como el proceso de reconocimiento (buscar y detectar potenciales reclutas) y posterior control y manipulación de los candidatos para lograr que estos sujetos internalicen una convicción política radical islamista, teniendo como propósito final el disponer de esos individuos radicalizados con la intención de participar en la yihad de una u otra manera.

PREÁMBULO. MECANISMOS DE RECLUTAMIENTO Y RADICALIZACIÓN YIHADISTAS

El ideario yihadista puede ser propagado a través de diversos canales: el adoctrinamiento llevado a cabo por las distintas organizaciones islámicas que operan en Occidente, material escrito o audiovisual (libros, vídeos), programas de televisión procedentes de países árabes, conversaciones de carácter privado mantenidas con el grupo de amigos bajo la batuta de un reclutador, o sermones ofrecidos por imanes radicales itinerantes en distintos países europeos con un amplio porcentaje de población musulmana.

Internet esta adquiriendo una progresiva importancia en lo referente a los mecanismos de reclutamiento y radicalización yihadistas. Así, a través de la red global los jóvenes musulmanes del mundo entero pueden tener acceso a la ideología yihadista, protagonista indiscutible en miles y miles de páginas Web y foros de Chat. En el contexto descrito resulta necesario hacer especial referencia a determinadas organizaciones islámicas, las cuales en muchos casos actúan en Europa en un aparente marco de legalidad, difundiendo su mensaje tanto física como virtualmente a través de Internet (CANO PAÑOS, 2008).

Hay que decir que estas organizaciones islámicas de carácter radical han experimentado en los últimos años un destacable progreso al recurrir al medio de comunicación más moderno: Internet. Así, cualquier individuo puede tener fácil acceso a las páginas Web pertenecientes a estos movimientos religiosos, lugares donde los mismos realizan labores de captación y adoctrinamiento entre los fieles (CANO PAÑOS, 2008, 12).

De acuerdo al artículo "El Estado Islámico capta terroristas en dos meses" del diario La Vanguardia (MARTÍN DE POZUELO, 2015), afirma DOLORES DELGADO, fiscal coordinadora contra el terrorismo yihadista: "Desde que se inicia la captación hasta la incorporación al EI pasan dos o tres meses, la incorporación de las mujeres a este terrorismo es otra gran novedad, recientísima" (…). En muy pocos años en España hemos pasado de las células extremistas que se limitaban a dar apoyo logístico a otros grupos a un terrorismo global y exprés que crea nuevos terroristas en cuestión de meses y que crece exponencialmente con la intención de matar. Tanto es así, que en lo que llevamos de año ya hemos incoado más procedimientos que en todo 2014. Estamos ante un terrorismo novísimo, transformado por internet y por la irrupción del Estado islámico. Se trata de un fenómeno patológico que habla en muchos idiomas pues para combatirlo es imprescindible la colaboración internacional". Así describe el panorama terrorista DOLORES DELGADO, fiscal de la Audiencia Nacional, coordinadora de la lucha contra el terrorismo yihadista desde el 2007. Es la fiscal de la última redada realizada en Cataluña y la que preparó la acusación contra GADAFI en el Tribunal Penal Internacional de La Haya.

Con todo, en las últimas fechas se ha podido comprobar cómo jóvenes musulmanes asentados en Europa deciden llevar a cabo la yihad, sin que los mismos tengan vínculo alguno con un reclutador yihadista o una organización adscrita o afín al islamismo radical. Se trata en estos casos de jóvenes musulmanes que se radicalizan rápidamente mediante la lectura de determinadas páginas Web o la visita de determinados foros de Chat. Asimismo, la red global de Internet proporciona a estos sujetos los conocimientos necesarios tanto para desarrollar determinadas estrategias de ataque como para construir un artefacto explosivo con el que cometer un atentado, sin necesidad así de someterse a un

entrenamiento paramilitar en Afganistán[220] (CANO PAÑOS, 2008, 13).

La aparición de Internet ha jugado, como en epígrafes anteriores, un papel protagonista en la nueva orientación de estos grupos a la hora de captar y entrenar miembros. La posibilidad de colgar contenidos en una plataforma fácilmente accesible y sujeta a pocas censuras ha conllevado la aparición de manuales electrónicos en los que se explica detalladamente cómo cometer actos terroristas. Este fenómeno ha sido denominado por algunos autores como la creación de una "universidad abierta para la yihad", impresión confirmada por la multiplicidad tanto de documentos con contenidos específicamente terroristas como aquellos más genéricos que permiten obtener los mismos resultados. Es por todo ello que un gran sector del mundo del análisis de seguridad ve un mayor peligro real en este "*cyberplanning*" que en la propia posibilidad de atentados conducidos por el ciberespacio (SÁNCHEZ FRÍAS, 2016).

Durante la fase de pre-radicalizacion/autoidentificación (CANO PAÑOS, 2008), la red global de Internet es utilizada por el individuo principalmente como fuente de información sobre el islam, en todas sus variantes e interpretaciones, así como lugar para encontrar *online* a otros individuos que se encuentran en la misma situación. Es evidente que aquel sujeto inmerso en la búsqueda de "respuestas" a las cuestiones vitales que se plantea se ve invariablemente expuesto a una plétora de interpretaciones del Islam de carácter extremista a las que puede tener acceso a través de Internet. Con el tiempo, estos jóvenes comienzan a visionar vídeos sobre la yihad, así como a asistir a conferencias y encuentros de carácter privado donde se suele ensalzar la guerra santa contra los infieles. También participan en distintos foros de Chat, lugares donde también se suele discutir sobre la yihad. Estas discusiones a través de la red permiten a muchos jóvenes musulmanes ir desarrollando una postura positiva hacia el Islam radical.

[220] Un ejemplo que confirma esta aseveración viene constituido por el caso de los dos jóvenes libaneses que en verano de 2006 intentaron cometer un atentado terrorista en Alemania mediante la colocación de bombas en trenes de cercanías. En este caso concreto, la protesta mundial contra las caricaturas de Mahoma publicadas en un diario danés actuó como "catalizador" para que ambos jóvenes decidieran llevar a cabo la yihad en territorio germano, sin que los mismos tuvieran vínculo alguno con una organización terrorista ni se hubieran sometido a un clásico proceso de radicalización. Por el contrario, la red global de Internet actuó como mecanismo de radicalización y "manual de instrucciones de la yihad" para ambos sujetos.

III.2.2.- Amenazas a personas o patrimonio

Delitos de calumnias e injurias, usurpación de identidad y revelación de secretos. La normativa europea - Directiva del Parlamento Europeo ydel Consejo relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo (2015) describe los delitos ligados a actividades terroristas como de extrema gravedad, ya que pueden conducir a la comisión de delitos de terrorismo y no se debe permitir que los terroristas y grupos terroristas mantengan y sigan desarrollando sus actividades delictivas, justificando la tipificación penal de dicha conducta.

Entre los delitos relacionados con la provocación a la comisión de un delito de terrorismo comprenden, entre otros, el enaltecimiento y la justificación del terrorismo o la difusión de mensajes o imágenes, en particular en relación con las víctimas del terrorismo, con objeto de publicitar la causa de los terroristas o de intimidar gravemente a la población, siempre que dicho comportamiento conlleve el riesgo de que se cometan actos terroristas[221]:

1. Todos los Estados miembros adoptarán las medidas necesarias para garantizar que los actos dolosos a que se refiere el apartado 2, tipificados como delitos según los respectivos Derechos nacionales y que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional, constituyan delitos de terrorismo cuando su autor los cometa con uno o varios de los siguientes objetivos:

    a. Intimidar gravemente a una población;
    b. Obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo;
    c. Desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o

[221] EUROPEAN COMMISSION. (2015). Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra el terrorismo, y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo.

sociales de un país o de una organización internacional.

2. Los actos dolosos a que se refiere el apartado 1 son los siguientes:

   a. Atentados contra la vida de una persona que puedan tener resultado de muerte;
   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 interrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas;
   i. Amenaza de ejercer cualquiera de las conductas enumeradas en las letras a) a h).

Teniendo en cuenta la evolución de las amenazas terroristas y las obligaciones legales de la Unión y de los Estados miembros en virtud del Derecho internacional, conviene aproximar en mayor medida la definición de los delitos de terrorismo, incluidos los delitos relativos a un grupo terrorista y los ligados a actividades terroristas, en todos los Estados miembros, de modo que abarque de forma más exhaustiva las conductas asociadas, en particular, a los combatientes

terroristas extranjeros y a la financiación del terrorismo. Estos tipos de comportamiento deberían ser igualmente punibles si se cometen a través de Internet, incluidos los medios sociales.

La Unión Europea y varias de sus directivas sobre las victimas del terrorismo:

Las víctimas del terrorismo requieren unas medidas de protección, apoyo y asistencia que respondan a sus necesidades específicas. En particular, deben tener acceso inmediato a servicios profesionales y especializados de apoyo que ofrezcan tratamientos físicos y psicosociales. Tras producirse un atentado terrorista, resulta fundamental facilitar una información fiable a las víctimas del terrorismo y sobre dichas víctimas. Dado que los atentados terroristas se dirigen contra grandes grupos de personas, es posible que, a menudo, las víctimas procedan de países distintos del que ha sufrido el atentado. Así pues, con vistas a garantizar que todas las víctimas del terrorismo estén bien informadas y reciban la asistencia necesaria con independencia del lugar de la Unión Europea en el que vivan, resulta esencial la cooperación transfronteriza entre las autoridades nacionales competentes.

La Directiva 2012/29/UE[222] establece un conjunto de derechos inalienables para todas las víctimas de delitos, entre ellos derechos a la protección, al apoyo y a la asistencia que tienen en cuenta las necesidades individuales de cada víctima de un delito. No obstante, estas disposiciones no prevén medidas específicas para las víctimas del terrorismo. La adopción de medidas más concretas que respondan de forma más precisa a las necesidades de las víctimas del terrorismo aportaría un considerable valor añadido. Es preciso complementar el proceso de sanación de las víctimas supervivientes y de las familias de las víctimas mortales y, por ende, de forma indirecta, el proceso de sanación del conjunto de las sociedades, con normas debidamente adaptadas en materia de protección, apoyo y asistencia a las víctimas del terrorismo.

[222] EUROPEAN UNION. (25 de octubre de 2012). Parlamento. Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la Decisión marco 2001/220/JAI del Consejo, de 15 de marzo de 2001 (*DO L* 315 de 14.11.2012, p. 37).

NEUMAN[223] define a la víctima como el ser humano que padece un daño en los bienes jurídicamente protegidos (la vida la salud, propiedad, honor, honestidad, etc.), por el hecho de otro e incluso por accidentes debidos a factores humanos, mecánicos o naturales, como ocurre en accidentes de trabajo. Podemos definir a la víctima del delito como aquella persona que sufre una afectación directa a sus derechos, por otro individuo, en bienes jurídicamente protegidos por la ley penal, Ahora bien es importante considerar a la victimología como toda disciplina científica y definir sus principales conceptos que se utilizan en su aplicación. Los cuales han trascendido en materia jurídica, consiguiendo alcanzar su terminología propia y reafirmar su propia identidad.

EL Parlamento Europeo y el Consejo de la UE, en su directiva 2012/29/UE, entienden por «víctima»:

a. La persona física que haya sufrido un daño o perjuicio, en especial lesiones físicas o mentales, daños emocionales o un perjuicio económico, directamente causado por una infracción penal.
b. Los familiares de una persona cuya muerte haya sido directamente causada por un delito y que haya sufrido un daño o perjuicio como consecuencia de la muerte de dicha persona.

Por tanto, la Comisión Europea (2015) menciona: los Estados miembros deben adoptar medidas específicas de protección, apoyo y asistencia que respondan a las necesidades especiales de las víctimas del terrorismo, mediante una mayor concreción y profundización de los derechos ya contenidos en la Directiva 2012/29/UE del Parlamento Europeo y del Consejo[224]. Se entenderá por “víctimas del terrorismo” las definidas en el artículo 1 de la Directiva 2012/29/UE, en relación con los delitos de terrorismo contemplados en el artículo 3. Las medidas que han de tomar los Estados miembros deben garantizar que, en caso de producirse un atentado terrorista, las víctimas del terrorismo obtengan un apoyo emocional y psicológico que comprenda ayuda para la superación del trauma y asistencia psicosocial, así como cualquier otra información y asesoramiento pertinente de carácter jurídico, práctico o financiero.

[223] Vid. LÓPEZ GARCÍA, L. Y. (2016). Ob., cit.
[224] Ibídem., p. 10.

Para CORONADO[225], los ataques ciberterroristas puede clasificarse de diversas formas. Entre éstas encontramos:

Tipos de ataques:

1. Simples: son los ataques orquestados contra sistemas en específico mediante herramientas creadas por otros. Son utilizados por grupos pequeños que no cuentan con grandes recursos y sus objetivos son menores.
2. Avanzados: son aquellos en los que organizaciones más estructuradas pueden atacar diversos sistemas y crear herramientas básicas para ello.
3. Complejos y coordinados: ataques ejecutados por organizaciones en contra de sistemas más sofisticados con herramientas propias y consecuencias mayores.

Ataques cibernéticos ejecutados con propósitos terroristas:

1. Incursión: ataques con la intención de acceder en un sistema o red para obtener o modificar información.
2. Destrucción: al acceder a una red o sistema y destruir información puede conllevar a diversas consecuencias como daños económicos.
3. Desinformación: ataques que pueden tener consecuencias inmediatas, ya que al clonar páginas de Internet o usuarios dentro de una red se puede difundir información errónea y generar caos.
4. Denegación de servicio: ataque con el que se sobrecarga un servidor para que los usuarios (legítimos) no puedan tener acceso a los servicios prestados.

Ampliando la línea terrorista y volviendo a los ciberataques, ROVIRA DEL CANTO (2011) nos presenta otras 2 categorizaciones, el *hacking* y el *groming,* además veremos el *Pishing,* la incitación a la xenofobia, odio racial y discriminación y los delitos relacionados con el patrimonio:

[225] CORONADO CONTRERAS, J. E. (7 de febrero de 2015). Breves consideraciones sobre la ciberdelincuencia y el ciberterrorismo. *Unión de Revistas de Estudiantes de Derecho URED*. Recuperado de: http://www.ured.org.mx/ured/breves-consideraciones-sobre-la-ciberdelincuencia-y-el-ciberterrorismo/

HACKING. Acceso ilícito sin autorización:

El término *"hacking"* tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje. De aquí la necesidad de su tratamiento autónomo y, además, en una configuración como el ilícito básico de casi todas las restantes modalidades de delitos informáticos, incluyendo los del ámbito económico.

Las respuestas legales en el Derecho comparado lo han venido tratando en otras áreas, principalmente la de los delitos contra la intimidad. Tales acciones suponen ataques contra bienes individuales y colectivos, sin necesidad de una posterior vulneración de la propiedad intelectual, industrial, o la existencia de un perjuicio económico o patrimonial efectivo, o un ánimo específico de atentar contra tales bienes jurídicos tradicionales.

El Hacking representa gravedad del riesgo y peligro que supone tal conducta o acción no sólo para el ámbito patrimonial y de la intimidad de la víctima, sino también para el preciso grado de fiabilidad y confianza de la sociedad, de la colectividad social, en la seguridad, seriedad, y veracidad de los datos, la información y los medios y redes por donde se comunican, transfieren o captan.

GROOMING. Acoso sexual a menores:

"Child Grooming" (acoso infantil). Por acoso infantil hay que entender todo conjunto de "acciones deliberadas cometidas por un adulto, con el fin de ganarse la confianza de un menor, crear una conexión emocional y con ello lograr disminuir las inhibiciones o reticencias del menor, para iniciar una relación sexual, primero virtual y posiblemente después física".

El *child grooming* a través de las TIC se ha extendido significativamente por cuanto los conceptos de seguridad y privacidad en los jóvenes, han evolucionado. Así hay menos reticencias a compartir datos personales (70% perfil público, cuantos más amigos, mejor); ha cambiado el concepto de "conocido", deviniendo en otro totalmente aleatorio; y se explica asimismo en la forma en cómo se acercan

los menores a Internet (como una extensión de la vida real) y con reserva activa de sus acciones y contactos con sus padres y tutores, y en muchos casos incluso reserva pasiva de éstos a conocer los contactos, relaciones y movimientos de sus hijos en la Red. Y ello se refleja en un estudio del año 2010 de la red *EU Kids Online* que aseveraba tres notas fundamentales:

a) Que el 29% de los niños europeos de entre 9 y 16 años que usan Internet, se ha comunicado en el pasado con alguien que no conocía cara a cara previamente.
b) Que el 61% de los padres de niños/as que han conocido en la vida real personas contactadas online dicen que su hijo/a no lo ha hecho.
c) Que en España un 8%de los menores españoles en alguna ocasión han quedado cara a cara con alguien a quien sólo conocían previo contacto en Internet; siendo que un 20% de los menores aseguran contactar online con gente que no conocen en la vida real.

Esquemáticamente podemos diferenciar las siguientes fases sucesivas en el *grooming*:

a) Fase de amistad.
b) Toma de contacto, gustos, preferencias. Confianza.
c) Fase de relación.
d) Confesiones personales e íntimas. Consolidación.
e) Componente sexual.
f) Participación actos naturaleza sexual, fotografías, webcam.
g) Extorsión
h) Escalada de peticiones.
i) ¿Agresión?

El Código Penal español en 2015 modifica el artículo 183 bis, que tiene la siguiente redacción: «El que, con fines sexuales, determine a un menor de dieciséis años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de carácter sexual, aunque el autor no participe en ellos, será castigado con una pena de prisión de seis meses a dos años. Si le hubiera hecho presenciar abusos sexuales, aunque el autor no hubiera participado en ellos, se impondrá una pena de prisión de uno a tres años.

Se añade un artículo 183 ter, con el siguiente contenido: «1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. 2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años»[226].

Se añade un nuevo artículo 183 quater, con el siguiente contenido: «El consentimiento libre del menor de dieciséis años excluirá la responsabilidad penal por los delitos previstos en este Capítulo, cuando el autor sea una persona próxima al menor por edad y grado de desarrollo o madurez».

La regulación internacional de la pornografía infantil:

Se puede argumentar que la pornografía infantil es un problema multi-jurisdiccional y que sólo un enfoque global mediante leyes uniformes puede tener impacto sobre esta problemática, a fin de evitar que las diferentes posturas de las legislaciones nacionales sobre pornografía infantil permita que los perpetradores concentren sus esfuerzos en jurisdicciones con regulaciones inexistentes o más laxas.

Los tres principales instrumentos jurídicos internacionales que se ocupan de la pornografía infantil son el *Protocolo facultativo sobre la venta de niños, la*

[226] Vid. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Nº. 77, Sec. I. p. 27121.

prostitución infantil y la utilización de niños en la pornografía, el *Convenio sobre Ciberdelincuencia del Consejo de Europa* y el *Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual*. Estos tratados contienen definiciones específicas de delitos, así como disposiciones que exigen castigo para las conductas criminalizadas.

La *Convención sobre los Derechos del Niño* (CDN), tiene por objeto garantizar una amplia gama de derechos humanos para los niños, incluyendo derechos civiles, culturales, económicos, políticos y sociales, pero también incluye disposiciones relativas a la explotación sexual infantil. El artículo 34 de esta Convención establece claramente que los Estados partes deben tomar medidas preventivas para hacer frente a la explotación sexual y abusos sexuales de niños, llevando adelante las acciones de alcance nacional, bilateral y multilateral para prevenir la explotación de menores en espectáculos o materiales pornográficos.

El *Protocolo facultativo sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía* entró en vigor el 18 de enero de 2002 y define a la pornografía como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales", para luego exigir en su artículo 3 inciso 1 c) que los Estados Partes tipifiquen como delito la pornografía infantil, ya sea cometida en el país o en el extranjero y de forma individual u organizada, incluyendo la simple posesión, con un agregado, entre comas en la versión en español, que introduce la cuestión de la intención de una forma confusa, aunque hace suponer que se refiere a la posesión con intención de llevar adelante las conductas descriptas previamente en el mismo artículo e inciso. También hace un llamamamiento al establecimiento de responsabilidad, civil, administrativa o penal, para las personas jurídicas en el entendimiento que un enfoque integral sobre la cuestión requiere la participación de la industria. A tono con las razones de esta sección de trabajo, el artículo 10 inciso 1 se refiere a que, atendiendo al hecho de que la pornografía se distribuye fácilmente a través de las fronteras por vía telemática, la cooperación internacional se presenta como perentoria.

Siguiendo con esa línea y viendo la relativa facilidad con la que las tecnologías de la información y las comunicaciones permiten a los delincuentes actuar en diferentes jurisdicciones de aquellas de las víctimas de sus delitos, el Consejo de Europa estableció su *Convenio sobre la Ciberdelincuencia* (también conocido como el *Convenio de Ciberdelincuencia* y aquí usado en forma indistinta, también en adelante el *Convenio*) con la esperanza de implementar un enfoque cooperativo y uniforme para el enjuiciamiento de los delitos cibernéticos. El *Convenio de Ciberdelincuencia* está abierto a la firma por los Estados miembros de Europa y los Estados no miembros que han participado en su elaboración, y a la adhesión de otros Estados no miembros.

Dentro del Título 3, *Delitos relacionados con el contenido*, el artículo 9 del *Convenio*, en su inciso 1, establece la obligatoriedad de los Estados Partes de tipificar la producción de pornografía infantil para la distribución a través de un sistema informático, el ofrecer o poner a disposición pornografía infantil a través de un sistema informático, el distribuir o transmitir pornografía infantil a través de un sistema informático, el adquirir pornografía infantil a través de un sistema informático para uno mismo o para otra persona y el poseer pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. Es importante aquí ver como la sola posesión está efectivamente tipificada como delito.

El inciso 2 del mismo artículo define a la pornografía infantil como todo material pornográfico que represente de manera visual a un menor participando en una conducta sexualmente explícita, a una persona que parezca ser un menor de edad participando en una conducta sexualmente explícita, y o a imágenes realistas que representen a un menor de edad involucrados en una conducta sexualmente explícita.

En línea con la *Convención de los Derechos del Niño*, el artículo 9 inciso 3 del *Convenio* dice que el término menor debe incluir a todas las personas menores de 18 años de edad, aunque dando la posibilidad de que un Estado Parte establezca una edad menor, que no podrá ser inferior a los 16 años.

Los artículos 11, 12 y 13 se ocupan de la cuestiones de la tentativa y complicidad, la responsabilidad de las personas jurídicas y de las penas,

respectivamente, finalizando la parte que nos interesa con el artículo 23 referido a la cooperación internacional.

El mismo Consejo de Europa estableció la *Convención para la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual*, también conocida como la *Convención de Lanzarote*, un tratado internacional que se centra en garantizar el interés superior de los niños a través de la prevención del abuso y la explotación, la protección y asistencia a las víctimas, el castigo a los autores, y la promoción de la cooperación nacional e internacional. Esta Convención se abrió a la firma el 25 de octubre de 2007 y entró en vigor el 1 de julio de 2010, estando abierta a la firma de los Estados miembros, los Estados no miembros que han participado en la elaboración de la Convención, la Comunidad Europea y la adhesión de otros Estados no miembros.

Con respecto a la pornografía infantil la *Convención de Lanzarote*, en su artículo 20 inciso 1 exige a los Estados Partes tipificar como delito la producción de pornografía infantil, el ofrecimiento o puesta a disposición de pornografía infantil, la distribución o transmisión de pornografía infantil, el procurar pornografía infantil para uno mismo o para otra persona, la posesión de pornografía infantil y el acceso, con conocimiento, a pornografía infantil a través de tecnologías de la información y de la comunicación.

La pornografía infantil es definida como “cualquier material que represente de manera visual a un niño en una conducta sexualmente explícita real o simulada o cualquier representación de los órganos sexuales de un niño con fines primordialmente sexuales” y se recomienda a los Estados Partes a adoptar legislación penalizando las actividades de reclutar o coaccionar a un niño para que sea parte de actividades de pornografía infantil o con conocimiento asistir a representaciones de pornografía infantil.

Al igual que el *Convenio sobre la Ciberdelincuencia*, la *Convención de Lanzarote* refiere a las cuestiones de tentativa y complicidad, responsabilidad de las personas jurídicas y cooperación internacional.

Se modifica el artículo 189, con el siguiente tenor literal:

«1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.
b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido. A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:
    - Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.
    - Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.
    - Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes[227].

[227] Vid. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Nº. 77, Sec. I. p. 27123.

- Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.
b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio.
c) Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.
d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.
e) Cuando el material pornográfico fuera de notoria importancia.
f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.
g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.
h) Cuando concurra la agravante de reincidencia.

3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años. La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español. Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal»[228].

PISHING. Robo de identidad:

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo (ilustración 35). El delito consiste en obtener

[228] Vid. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado (BOE).*Nº. 77, Sec. I. p. 27121.

información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños[229].

Ilustración 35: *Ladrones de identidad.*

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

Incitación a la xenofobia, odio racial y discriminación:

Con la reciente reforma del Código Penal en España, muchas de las ciberconductas que se producían en internet han pasado a formar parte del catálogo de delitos recogidos por la Ley. En el artículo 510, se habla del fomento, promoción o incitación directa o indirectamente al odio, hostilidad, discriminación o violencia contra las personas, previendo el supuesto desi se realiza a través de

[229] ACURIO DEL PINO, S. (2011). Delitos informáticos: generalidades. (OEA) Jurídica Cono Sur. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

internet, es por este motivo que conviene analizarlo[230].

- Artículo510 CP de España.

Apartado: De los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución.

Características: Se castiga con una pena de prisión de 1 a 4 años y multa de 6 a 12 meses:

- A quien realice públicamente el fomento, promoción o incitación directa o indirectamente al odio, hostilidad, discriminación o violencia contra las personas por motivos:

  - Racistas.
  - Antisemitas.
  - Ideología, religión o creencias.
  - Situación familiar.
  - La pertenencia a una etnia, raza o nación, su origen nacional.
  - Sexo, orientación o identidad sexual.
  - Razones de género, enfermedad o discapacidad.

- A quien produzca, elabore, posea con la finalidad de distribuir, facilite a terceros el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para realizar las acciones anteriores.

- A quien públicamente niegue, trivialice gravemente o enaltezca los delitos de genocidio, de lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, o enaltezcan a sus autores, cuando se hubieran cometido por los motivos anteriores, cuando de este modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra las personas.

[230] Ciberderecho (2015). El nuevo artículo 510 del código Penal de España. Recuperado de: http://www.ciberderecho.com/el-nuevo-articulo-510-del-codigo-penal-de-espana/

Adicionalmente, se castiga con la pena de prisión de 6 meses a 2 años y multa de 6 a 12 meses:

- A quien lesione la dignidad de las personas mediante acciones que entrañen humillación, menosprecio o descrédito de alguno de los grupos anteriores.

- A quien produzca, elabore, posea con la finalidad de distribuir, facilite a terceros el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para realizar las acciones anteriores por que además represente una grave humillación, menosprecio o descrédito de alguno de los grupos mencionados.

- A quien enaltezca o justifique por cualquier medio los delitos que hubieran sido cometidos, o a quienes hayan participado en su ejecución, contra las personas por los motivos anteriormente citados.

Los hechos serán castigados con una pena de 1 a 4 años de prisión y multa de 6 a 12 meses cuando de ese modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra los mencionados grupos.

Penas adicionales por uso de internet:

Las penas 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.

Para estos casos, el juez o tribunal acordará la destrucción, borrado o inutilización del material de soporte objeto del delito a que se refieren los apartados anteriores o por medio de los cuales se hubiera cometido. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación, se acordará la retirada de los contenidos.

Delitos relacionados con el patrimonio:

Entre estas encontramos las siguientes conductas principales (ROMEO CASABONA (s. f.):

- Accesos no autorizados no consentidos en ficheros, bases de datos o sistemas informáticos ajenos *(hackering)*, los cuales pueden perseguir los más variados objetivos y una dañosidad también de muy diversa entidad: desde las acciones destructivas *(crackering),* pasando por lo que se conoce como "intromisión blanca", expresión con la que se designa el supuesto de hecho conforme al cual en realidad no se persigue un propósito diferente a lograr el mero acceso a un archivo o base de datos por lo general protegido por procedimientos lógicos (informáticos) concebidos para impedir accesos de terceros no autorizados.

- Interceptaciones de las comunicaciones: Son asimismo relevantes desde el punto de vista jurídico-penal las interceptaciones de las comunicaciones de carácter personal o de otra naturaleza (financiera, comercial, etc.), como pueden ser los mensajes de correo electrónico, conversaciones orales o escritas a tiempo real (teléfonos por cable, celulares o móviles, foros restringidos, chat), remisión o intercambio de documentos, etc.

- Manipulaciones de datos o de sistemas informáticos: Por otro lado, también pueden realizarse modificaciones, incluso meramente transitorias, mediante manipulaciones de datos o de sistemas informáticos con el fin de obtener un beneficio, por lo general económico.

- Interferencias dañosas o inutilizadoras de sistemas informáticos: Son igualmente demasiado conocidas las difusiones de virus informáticos y la perpetración de otras conductas dañosas o inutilizadoras de los sistemas informáticos y de ficheros a través de la red (daños sabotaje informático, ciberterrorismo), los cuales suelen expandirse con gran rapidez y amplitud en todo tipo de terminales, incluidos los de uso doméstico o personal, para cuyo propósito se utiliza con frecuencia el correo electrónico o las descargas de contenidos de la red como medios transmisores y de acceso al sistema del terminal, pudiendo alcanzar sus daños globales en ocasiones cuantías

económicas muy elevadas.

- Introducción y difusión en la red de contenidos ilícitos: La posibilidad de introducir información (datos, imágenes, voz y sonido) en la red con contenidos ilícitos muy diversos y de difundirlos a través de aquélla, han convertido a la red en un medio muy potente para la comisión de otros delitos: apología del terrorismo y de otros actos preparatorios relacionados con él, incitación a la xenofobia, al odio racial y a la discriminación, escarnio religioso, difusión y posesión de pornografía infantil.
- Copia e intercambio de obras de creación intelectual.
- Accesos no autorizados.
    - "El aumento de los *exploit kit* se revela con *Rig EK*, segunda amenaza a nivel mundial en Marzo"[231]. Los exploits son uno de los mayores problemas referentes a la seguridad de datos y sistemas, estos son un tipo de malware que nos puede atacar a través del contacto con alguna pagina web a través del navegador o bien abriendo algún archivo infectado que nos llega a través de algún spam, estos se encargan de analizar nuestro software y sistema y detectar nuestra vulnerabilidades para de esta forma poder manejar nuestro sistema, estos se caracterizan porque se pueden explotar con mínimos conocimientos técnicos y están al alcance de cualquier usuario medianamente avispado.

III.2.3.- Adoctrinamiento de personas

Respecto a Internet y las redes, tras los atentados de París, el primer ministro francés insistió en que éstas cada vez son más utilizadas para el "adoctrinamiento" y "la captación" de futuros yihadistas, así como para difusión de "mensajes de odio". También para que los terroristas contacten entre ellos" y para la adquisición de técnicas que luego les permiten pasar a la acción"[232].

[231] INCIBE (Mayo de 2018). Instituto Nacional de Ciberseguridad. Cibercrime: Concept, Types and State.

[232] YÁRNOZ, C. (13 de enero de 2015). Valls anuncia controles inmediatos sobre internet en la

GUTIÉRREZ[233] ejemplifica el caso de un marroquí detenido en Murcia en 2014, quien escribió en Facebook: "en tiempos en que los infieles y los tiranos invaden nuestra nación, la yihad y la lucha armada son la elección y el camino (...) En cuanto nos levantemos en armas, al enemigo le entrará miedo y su sangre será derramada", como promoción del yihadismo.

A menudo se atribuye a internet y a las redes sociales una importancia decisiva en el proceso de radicalización yihadista (GUTIÉRREZ, 2016). Sin embargo, en España sólo el 18.4% se sumó al Estado Islámico (EI) exclusivamente por esa vía, siendo *Facebook, Youtube* y *Twitter* las plataformas más utilizadas. El 28.9% se integró por vía off-fine, es decir, de manera presencial en domicilios privados, lugares de culto o centros culturales islámicos, espacios al aire libre y, en menor medida, en centros penitenciarios. En realidad, la mayoría (52.7%) se radicalizó en un "entorno mixto": internet y la opción presencial.

La razón por la que se unen, añade, principalmente (62.8%) es por razones "ideológicas y utilitarias" en las que se justifica el terrorismo, como lo ofrecía el cabecilla de la Brigada Al-Ándalus a sus seguidores: "Es una obligación hacer la yihad y hay muchos hermanos que han ido a la yihad", o la vía "utilitaria", que refiere a la yihad como opción ante la interpretación de una hostilidad generalizada hacia la comunidad de los creyentes del Islam.

La Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra el terrorismo, y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo[234] (COMISIÓN EUROPEA, 2015) considera que los grupos terroristas han demostrado competencias avanzadas en cuanto a la utilización de Internet y de las nuevas tecnologías de comunicación para difundir propaganda, interactuar con posibles adeptos, compartir conocimientos, planificar y coordinar operaciones. En particular, Internet y los medios sociales han brindado a los grupos radicales y terroristas nuevas oportunidades de llegar a públicos vulnerables y facilitar, de este modo, la captación o la autorradicalización. El

lucha antiyihadista. *El Pais*. Recuperado de: http://internacional.elpais.com/internacional/2015/01/13/actualidad/1421145961_694800.html

[233] GUTIÉRREZ, A. (18 de agosto de 2016). Quiénes son y cómo se enrolan los yihadistas. *Periódico digital proceso.com.* Recuperado de: http://vlex.com/vid/enrolan-yihadistas-647106597

[234] Vid. EUROPEAN COMMISSION. (2015). Ob., cit.

empleo de material de comunicación de alta calidad (revistas, vídeos) y de un enfoque descentralizado favorecido por una red de cuentas en una serie de plataformas de medios sociales permite la rápida difusión de contenidos radicales y terroristas a través de la continua adaptación del uso de las tecnologías de la información. Internet se ha convertido en el principal canal utilizado por los terroristas para difundir propaganda, publicar amenazas, ensalzar terribles actos terroristas tales como las decapitaciones, y reivindicar la autoría de atentados.

Para CANO[235], la fase de adoctrinamiento por parte de los reclutadores islamistas se centra en tres pilares fundamentales:

En primer lugar, los "representantes" de la yihad sólo necesitan hacer referencia a las razones que, en su opinión, conllevan a que estos jóvenes sean empujados hacia una marginalidad social. Tanto su origen étnico, su religión, su estatus social, el barrio en el que habitan…Todos estos factores impiden, según ellos, que esos jóvenes musulmanes puedan ser aceptados y reconocidos como ciudadanos de pleno derecho por parte de la sociedad autóctona mayoritaria.

En segundo lugar, es durante esta fase cuando los individuos que están siendo radicalizados son expuestos gradualmente a una propaganda acerca de las –percibidas– injusticias al pueblo musulmán en todo el mundo en el marco de unos conflictos de carácter internacional, los cuales son interpretados unilateralmente como ejemplos de una guerra generalizada de Occidente en contra del Islam. Desde el conflicto de Cachemira hasta la invasión norteamericana de Iraq, todos estos acontecimientos son interpretados por estos jóvenes musulmanes como un ataque, como una conspiración de los infieles contra el Islam y contra el mundo musulmán en general. De este modo, estos sujetos consideran que la mal llamada "guerra contra el terrorismo" es en realidad un silogismo utilizado por Occidente para enmascarar una guerra que se está librando contra el Islam.

En tercer lugar, es en la fase de adoctrinamiento cuando aparece el tema del Islam real y puro. Para los reclutadores yihadistas, esta particular y tergiversada visión del Islam defendida por ellos es el tema fundamental que debe

[235] CANO PAÑOS, M. Á. (2008). Ob., cit.

centrar la vida de los jóvenes candidatos.

Durante la etapa de adoctrinamiento, aquellos sujetos que están sufriendo ese "lavado de cerebro" por parte de los reclutadores yihadistas dedican su tiempo a navegar por el ciberespacio a la búsqueda de páginas Web de carácter extremista y foros de Chat donde encuentran a otros sujetos afines ideológicamente. Ambos instrumentos le refuerzan al recluta su ideología y compromiso con la yihad. Además, los reclutadores yihadistas les muestran vídeos propagandísticos en los que se muestran las "injusticias" que se están llevando a cabo contra la población musulmana en países como Iraq, Chechenia o Palestina. En no pocas ocasiones, son los propios jóvenes los que tienen acceso a ese material a través de Internet. Así, programas informáticos de mensajería instantánea como por ejemplo Paltalk permiten reunir online a cientos de jóvenes musulmanes, muchos de ellos embarcados ya en un proceso de radicalización. En dichos foros suelen mostrarse desde vídeos donde se decapita a un rehén en Iraq hasta instrucciones prácticas de estrategia y combate para los futuros mujahedines. Además, hay que destacar que los reclutadores yihadistas activos online no sólo centran su atención en los jóvenes musulmanes asentados en países como Afganistán, Pakistán o Palestina, sino que primordialmente se dirigen a las segundas y terceras generaciones de inmigrantes musulmanes que habitan en Occidente. Sin ir más lejos, la página Web conocida como "El Frente Global de Medios de Comunicación Islámico"[236] presenta sus contenidos en alemán desde finales de 2006. En la mencionada página Web, el internauta tiene a su disposición una especie de "*Best of terrorism*", con los últimos atentados, secuestros o decapitaciones cometidos en Iraq o Afganistán en nombre de Allah, o las últimas proclamas emitidas por los altos dirigentes de Al Qaeda. Mientras que esos vídeos hacen añicos la (aparente) sensación de seguridad de Occidente, por otra parte, transmiten a los islamistas repartidos por todo el mundo un sentimiento de unión, de pertenencia a una comunidad de creyentes y de superioridad (CANO PAÑOS, 2008).

[236] Vid. Instituto de investigación de medios del Medio Oriente (MEMRI). Recuperado de: https://www2.memri.org/espanol/el-frente-global-de-medios-de-comunicacion-islamico-al-qaeda-en-irak-ha-reemplazado-a-la-organizacion-madre-en-afganistan-y-esta-esparciendo-el-jihad-a-lo-largo-del-mundo/1046

En la fase yihadista, los yihadistas utilizan la red global de Internet no sólo para realizar labores de captación, reclutamiento y adoctrinamiento, sino también para formar células o grupos con la intención de cometer atentados terroristas. Se trata de sujetos procedentes de países distintos, individuos que ni siquiera se conocen personalmente, ni se han visto nunca. No obstante, la red permite que ese grupo de carácter virtual adquiera con el tiempo realidad física, llegando a desencadenar una violencia inusitada (CANO PAÑOS, 2008, 18).

III.2.4.- Enaltecimiento y justificación

El enaltecimiento/justificación, tratado en el art. 578CP vigente, constituye una forma autónoma de apología caracterizada por su carácter genérico y sin integrar una provocación ni directa ni indirecta a la comisión de un delito. La barrera de protección se adelanta, exigiéndose solamente la mera alabanza/justificación genérica, bien de los actos terroristas o de quienes los efectuaron". Para reforzar esta teoría de la sustantividad de esta específica apología "*in genere*", se incide en el argumento de que su respuesta punitiva es también autónoma e independiente, frente a las apologías "clásicas" de los arts. 18 y 579 en las que la pena lo es por referencia a la que corresponda al delito a cuya ejecución se incita *jus ad bellum (*AGUDO FERNÁNDEZ, PERRINO PÉREZ, & JAÉN VALLEJO, 2016).

El análisis de PONTE (2015) puede resumir y explicar este delito como sigue:

Art. 578.- ENALTECIMIENTO Y HUMILLACIÓN DE LAS VÍCTIMAS

Conducta tipificada:

- Enaltecimiento o justificación de los delitos de terrorismo
- Las personas que hayan cometido actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos de terrorismo o de sus familiares.

Penalidad: Prisión 1-3 años y multa 12-18 meses y prohibiciones art. 57. Agravación:

- Mitad superior: Difusión a través de medios de comunicación, internet u

otras tecnologías.

- Mitad superior hasta superior en grado: mensajes o actos Idóneos para alterar paz pública o crear sentimiento de inseguridad o temor en la sociedad.

MEDIDAS CAUTELARES (durante la instrucción) O DEFINITIVAS (en sentencia):

Destrucción, borrado o inutilización de libros, archivos, documentos o cualquier soporte; retirada de contenidos (si es mediante internet o similares); supresión de enlaces; y bloqueo de acceso a esos contenidos.

La exaltación del terrorismo ha venido a sustituir en la última reforma a la apología, que planteó problemas de inconstitucionalidad. Castiga el art. 579 el enaltecimiento o la justificación de los delitos de terrorismo o de quienes hayan participado en su ejecución por cualquier medio de expresión pública o difusión. También se incluye en la exaltación del terrorismo la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares. La pena prevista es la de prisión de uno a dos años (así como algunas de las restricciones de libertad -particularmente en cuanto al acercamiento a las víctimas- recogidas por el art. 47 CP).

Para SÁNCHEZ FRÍAS (2016), el auge de Internet, con su fácil acceso y bajo coste, ha eliminado casi por completo esta traba que se presentaba a las organizaciones terroristas. El avance de las nuevas tecnologías, aunque proporciona grandes beneficios para la sociedad en general, también ha permitido que la mayoría de grupos terroristas mantengan sitios webs propios en los que se contienen, entre otros, datos sobre su historia y principales éxitos. Los datos, recopilados y presentados para el público objetivo, son incluso traducidos en diferentes lenguas para que los ciudadanos extranjeros puedan comparar los puntos de vista terroristas con los ofrecidos por los medios de comunicación.

Teniendo en cuenta el objetivo propagandístico, las páginas web patrocinadas por grupos terroristas para cometer atentados no suelen, por lo general, realizar un enaltecimiento injustificado de la violencia empleada. Al contrario, presentan su situación como la respuesta de la oposición política a

ataques extranjeros contra su libertad de expresión para así poder atraer la empatía de los defensores occidentales de las libertades civiles. Y qué mejor medio para hacerlo que Internet, considerado máximo símbolo de la libertad de expresión sin censuras. En esta línea se han identificado tres estructuras comunes en estas webs a la hora de justificar esta violencia:

La primera de las estructuras mencionadas anteriormente consiste en presentar la violencia como única respuesta posible ante la opresión del enemigo, calificando las actuaciones estatales como "asesinatos" o "genocidios". La segunda, en maximizar la actuación del enemigo para legitimar así la violencia empleada por el grupo terrorista como un acto de defensa frente a una agresión, autodenominándose "luchadores de la libertad". Y, por último, emplear el lenguaje de la no violencia cuando confirman la búsqueda pacífica de soluciones y solicitan la presión internacional ante un gobierno represivo. La importancia de estos contenidos en plataformas virtuales no debe despreciarse, máxime teniendo en cuenta la situación actual de crecimiento del número de "combatientes extranjeros" incorporados al Estado Islámico (SÁNCHEZ FRÍAS, 2016).

AGUDO[237] reconoce la tensión que existe entre este delito y el derecho a la libre expresión de ideas y libertad ideológica, como expresamente se admite por ejemplo en la Sentencia del Tribunal Supremo de 20 de junio de 2007[238]. La Sala Segunda nos indica en esta misma resolución que "la labor judicial, como actividad individualizada que es en un riguroso análisis, caso por caso, habrá de examinar tanto las concretas frases o expresiones producidas así como la ocasión y el escenario en el que fueron pronunciadas y, en fin, todas las circunstancias concurrentes, para determinar si está dentro del ámbito del tipo penal o extramuros de él, sin olvidar que el principio *favor libertatis* debe jugar, necesariamente en los casos de duda, ante la naturaleza constitucional de los derechos de libertad de expresión e ideológica que podrían quedar afectados por el tipo penal, derechos que constituyen una de las más acusadas señas de identidad de la Sociedad Democrática".

[237] AGUDO FERNÁNDEZ, E., PERRINO PÉREZ, Á. L., y JAÉN VALLEJO, M. (2016). Terrorismo en el siglo XXI. La respuesta penal en el escenario mundial. Madrid: Dykinson.

[238] Vid. Tribunal Supremo. Sala Segunda. (2007). Sentencia 585/2007, de 20 de junio; recurso 1303/2006. Ponente: Magistrado D. SIRO FRANCISCO GARCÍA PÉREZ.

"La Audiencia Nacional ha firmado 86 sentencias por enaltecimiento del terrorismo en España desde 2004 (ver ilustración 36), aunque el delito estaba tipificado desde 2000. De esas sentencias, el 59% acabaron en condena y el 41% en absolución. De las que acabaron en condena, la pena más habitual es de un año de prisión, que se produjo en 39 de las 51 sentencias condenatorias. Además, el Tribunal Supremo ha firmado otras 9 sentencias en segunda instancia por enaltecimiento del terrorismo". "La información obtenida del buscador de jurisprudencia revela que la mayoría de juicios por este delito fueron por la exhibición pública de pancartas, mensajes o fotografías de o sobre presos de la banda terrorista ETA. En total, casi la mitad fueron por esta razón (37 de las 86 sentencias). Así sucedió con dos personas que fueron condenadas en marzo de 2014 por la Audiencia Nacional a un año de prisión por un delito de "enaltecimiento del terrorismo", por portar en una manifestación dos fotografías de presos de ETA con la palabra "amnistía". Sin embargo, la mayoría de sentencias relacionadas con la exhibición de estos mensajes terminaron en absolución de los acusados"[239].

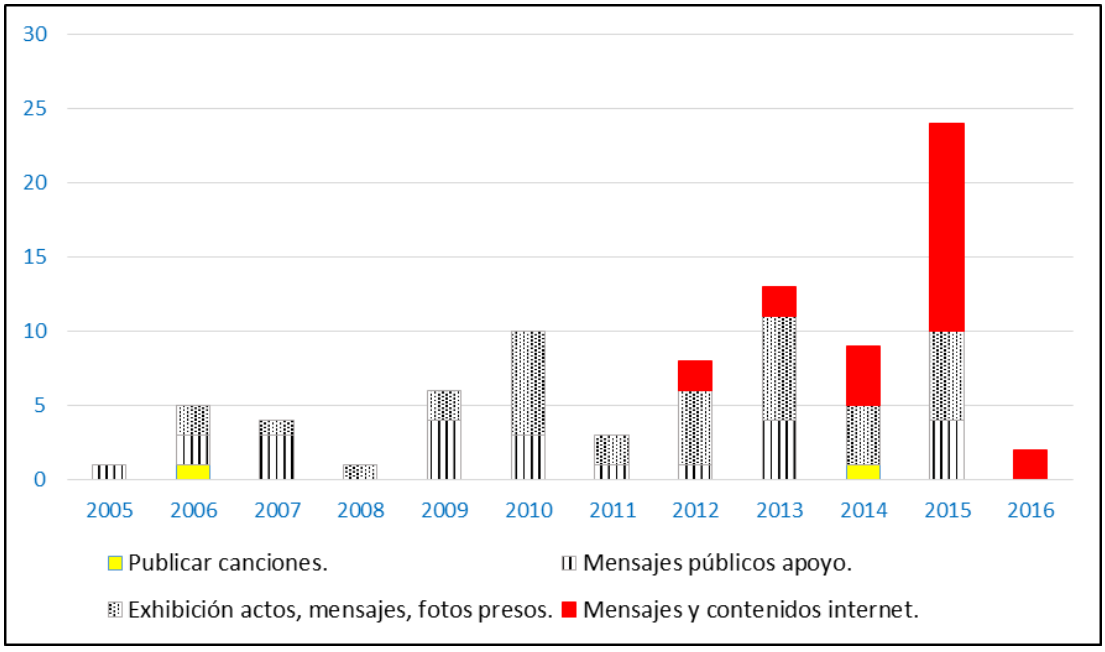


Ilustración 36: *Evolución del número de sentencias de la Audiencia Nacional por un delito de "enaltecimiento del terrorismo" 2005-2016*[240].

[239] El diario.es (12 de febrero de 2016). Nunca se ha juzgado a nadie en Españ por "enaltecimiento del terrorismo" en una obra de ficción. Recuperado de:https://www.eldiario.es/politica/titiriteros-Espana-enaltecimiento-terrorismo-ficcion_0_483652582.html

[240] Ibídem. CENDOJ, ´datos del gráfico Raúl Sánchez.

Puesto que no existe una zona intermedia entre la libertad de expresión como derecho universal y el delito de enaltecimiento totalmente clara, en relación a esa «zona intermedia», la Sentencia del Tribunal Supremo de 19 de febrero de 2015, señala que "el bien jurídico protegido estaría en la interdicción de lo que el TEDH–SSTEDH de 8 de julio de 1999, SÜREK vs Turquía y también nuestro Tribunal Constituciónal –STC 235/2007 de 7 de noviembre– califica como el discurso del odio, es decir la alabanza o justificación de acciones terroristas que no cabe incluirlo dentro de la cobertura otorgada por el derecho a la libertad de expresión o ideológica en la medida que el terrorismo constituye la más grave vulneración de los Derechos Humanos de aquella Comunidad que lo sufre, porque el discurso del terrorismo se basa en el exterminio del distinto, en la intolerancia más absoluta, en la pérdida del pluralismo político y en definitiva en la aterrorización colectiva como medio de conseguir esas finalidades" (AGUDO FERNÁNDEZ et. al, 2016).

Esas acciones de enaltecimiento tienen como objetivo final los potenciales miembros de una amplia campaña de propaganda que defiende los ideales de cada grupo concreto y les anima a formar parte de ello facilitándoles datos sobre cómo unirse a su causa. Esta movilización en casos como el Estado Islámico es de tal calibre que ha llegado, incluso, a compararse con la realizada a través de videojuegos y películas norteamericanas para animar a la población a unirse al ejército. A lo anterior hay que añadir que este reclutamiento no busca únicamente sumar miembros que cometan actos violentos, sino que también se dan una serie de pautas de comportamientos no violentos que pueden ayudar a la causa del grupo terrorista. Ejemplo de ello es el gran número de páginas web alrededor del mundo que se solidarizaron y elevaron protestas contra la detención de ABDULLAH OCALAN, líder del grupo terrorista kurdo PKK. Todos los casos expuestos hasta aquí demuestran el peso de los contenidos publicados en Internet a la hora de mantener el funcionamiento de los grupos terroristas en áreas tan diversas como la formación, el reclutamiento o la publicidad (SÁNCHEZ FRÍAS, 2016).

El enaltecimiento terrorista ha sufrido un endurecimiento inusitado con ocasión de los atentados en París, expresado en la última reforma CP que entró en vigor el 1 de julio de 2015. También vino precedido por un "pacto antiterrorista" entre los dos partidos mayoritarios del arco parlamentario. En este delito, descrito

como elogio hacia actos de terrorismo y/o como desprecio a sus víctimas, subyace un reproche moral hacia la opinión no alineada con el discurso oficial, absolutamente polarizado entre buenos y malos, que ya a estas alturas la mayoría de la gente ha optado por cuestionar. Respecto de las víctimas del terrorismo, se aprecia una reprobación por la ofensa que representa. En uno y otro caso lo que se castiga penalmente es la "ofensa" (GARCÍA, 2016).

Por lo que respecta al enaltecimiento, la Sentencia del Tribunal Supremo de 26 de febrero de 2007[241], recoge los elementos que vertebran este delito (AGUDO FERNÁNDEZ et., al, 2016):

1. La existencia de unas acciones o palabras por las que se enaltece o justifica.

   Por lo que respecta a enaltecer, equivale a ensalzar o hacer elogios, alabar las cualidades o méritos de alguien o de algo. Por lo tanto, aparece emparentado, aunque tiene un significado más amplio con el concepto de apología del párrafo II del artículo 18.1 C. P.

   En relación con el término justificar, quiere aquí decir que se hace aparecer como acciones lícitas y legítimas aquello que solo es un comportamiento criminal.

2. El objeto de tal ensalzamiento o justificación puede ser alguno de estos dos:

   a. Cualquiera de las conductas definidas como delitos de terrorismo de los arts. 571 a 577 (numeración en la fecha de los hechos).
   b. Cualquiera de las personas que hayan participado en la ejecución de tales comportamientos. Interesa decir aquí que no es necesario identificar a una o a varias de tales personas. Puede cometerse también ensalzando a un colectivo de autores o copartícipes en esta clase de actos delictivos.

3. La acción de enaltecer o justificar ha de realizarse por cualquier medio de expresión pública o difusión como puede ser evidentemente un periódico que se distribuye entre sus lectores cualquiera que sea la extensión de tal

[241] Tribunal Supremo, Sala Segunda (2007). Sentencia 149/2007, de 26 de febrero: recurso 11281/2006. Ponente: Magistrado D. Joaquín Delgado García.

distribución. Por lo que respecta al bien jurídico protegido no lo específica la doctrina y así hay quien considera que se trata de "la moral predominante en una sociedad", o "los sentimientos de perplejidad e indignación social" (AGUDO FERNÁNDEZ et., al, 2016).

III.2.5.- Provocación conspiración y proposición

Según el análisis del artículo del Servicio de Abogados (2015), son cuatro las conductas estudiadas bajo el nombre de resoluciones manifestadas: la conspiración, la proposición, la provocación y la apología, que es una forma de provocación[242]. El artículo realiza un análisis de cada una de ellas definiéndolas de la siguiente forma:

- **La conspiración** consiste en el plan ideado por varias personas para cometer un delito. Aunque es necesario que intervenga más de una persona, no lo es, sin embargo, que todas ellas participen en el delito de la misma manera. Unos pueden realizar la conducta y otros ayudarles a escapar, por ejemplo. Lo que sí es imprescindible es que todos los individuos tengan claro qué delito va a cometerse y con qué medios.

- **La proposición** para delinquir se dará cuando un sujeto haya decidido cometer un delito y, con posterioridad a dicha decisión, invite a otras personas a ejecutarlo junto con él. Aquí, al igual que en la conspiración, se requiere que participen varios sujetos, aunque la idea sólo provenga, en un principio, de uno de ellos.

- **La provocación** es la incitación directa a la perpetración de un delito hecha frente a un grupo de personas o utilizando medios de difusión que faciliten la transmisión del mensaje o propósito delictivo (la prensa, la radio, la televisión, internet, etc. (…). Debe tratarse de una provocación de cierta intensidad, susceptible de poder generar en los espectadores o destinatarios del mensaje

[242] SERVICIO DE ABOGADOS. (26 de abril de 2015). Las resoluciones manifestadas: La conspiración, la proposición, la provocación y la apología. Recuperado de: http://juiciopenal.com/delitos/las-resoluciones-manifestadas-la-conspiracion-la-proposicion-la-provocacion-y-la-apologia/

la voluntad o la decisión de cometer un delito. Si alguna de estas personas llegara efectivamente a delinquir, el provocador será considerado como inductor, con el consiguiente incremento de la pena (la misma que para el autor del delito).

El Código penal español (1995) define los anteriores términos tal como sigue:

- **Conspiración**

El artículo 17.1 CP[243] contiene la definición legal de conspiración: "*existe cuando dos o más personas se conciertan para la ejecución de un delito y resuelven ejecutarlo".*

La conspiración se ubica entre la ideación impune y las formas imperfectas de ejecución, y constituye una especie de coautoría anticipada[244]Nos hallamos ante la denominada coautoría anticipada, en la que se contempla la intervención de todos los conspiradores en la realización material del hecho delictivo, sea cual fuere el cometido o la parte del plan acordado que les haya tocado ejecutar a cada uno de los concertados[245].

Si se inicia la ejecución del delito, los hechos se castigarán como tentativa (forma imperfecta de ejecución) o como delito consumado, y no por conspiración, porque el desvalor de ésta se ve consumido por el de aquélla (principio de consunción). De esta manera, la jurisprudencia viene entendiendo que la conspiración, caracterizada por la conjunción del concierto previo y la firme resolución, es incompatible con la iniciación ejecutiva material del delito, que supondría ya la presencia de coautores o partícipes de un delito intentado o consumado[246].

La jurisprudencia viene exigiendo dos requisitos para que exista la conspiración para delinquir: en primer lugar, debe existir un *pactum scaeleris* o concierto previo; y, por otra parte, debe concurrir la resolución firme de cometer

[243] Vid. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la LeyOrgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado (B.O.E.) nº. 77. pp. 27061-27176. Vigencia: 1 julio 2015.

[244] Vid. Sentencia del Tribunal Supremo 321/2007 de 20 de abril.

[245] Vid. Sentencia del Tribunal Supremo 1994/2002 de 29 de noviembre.

[246] Vid. Sentencia del Tribunal Supremo de 7 de febrero de 2007, que cita la de 20 de mayo de 2003.

un delito o decisión seria de ejecución.

- **Proposición**

La proposición para delinquir, se define desde un punto de vista legal, como aquel acto preparatorio del delito, previo a la ejecución del mismo, correspondiente a la fase externa en la vida del delito, que consiste en la manifestación de voluntad del sujeto que ha resuelto cometer un delito, invitando a otra u otras personas a participar en él.

La incitación a delinquir, se define desde un punto de vista legal, como aquel acto preparatorio del delito, previo a la ejecución del mismo, correspondiente a la fase externa en la vida del delito, que consiste en la manifestación de voluntad del sujeto que directamente provoca, incita, por medio de imprenta, la radiodifusión o cualquier medio de eficacia semejante que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito.

La proposición se diferencia de la "inducción" en que ésta ha de ser eficaz, es una proposición aceptada y realizada, mientras que en la proposición el proponente tiene la resolución criminal, pero no es preciso que se la transmita al invitado, siendo compatible con que éste rechace la invitación. La proposición se diferencia de la incitación a delinquir, en que en la proposición ha resuelto cometer, material y personalmente, un delito, y trata de sumar a sus propósitos a otra u otras personas, constituyendo con ellos un grupo criminal (codelincuencia), mientras que en la incitación a delinquir el incitador no está resuelto a ser ejecutor del delito, a cuya perpetración incita, ni pretende que dicha perpetración sea conjunta, sino que se limita al intento de determinar a otro u otros a la participación en un delito, pero sin que él haya de tomar parte directa o material en la misma.

Entre las consideraciones pertinentes a este aspecto, cabe resaltar el análisis hecho por GABARI[247] quien plantea que "*ya no es necesario que los mensajes o consignas vayan dirigidos a provocar, alentar o favorecer la perpetración de delitos, ahora se cambia por que tengan como finalidad o que por*

[247] GABARI GÁMEZ, A. (2015). La regulación del terrorismo en el CP: Una regulación de excepción. Trabajo Fin de Grado Universidad Pública de Navarra. Recuperado de: http://academica-e.unavarra.es/bitstream/handle/2454/18400/72249TFGGabari.pdf?sequence=1&isAllowed=y

su contenido, sean idóneos para incitar a la comisión". De modo que se vuelven a adelantar las barreras punitivas. Se castiga al que de manera pública incite a otros a la comisión de los delitos del Capítulo VII y se incluye un subtipo atenuado, teniendo en consideración la gravedad del hecho, el medio empleado o el resultado producido.

Asimismo GABARI[248], expresa que "*Deben establecerse sanciones para las personas físicas que hayan cometido dolosamente delitos de provocación a la comisión de delitos de terrorismo, de captación y de adiestramiento de terroristas o para las personas jurídicas consideradas responsables de dichos delitos. Estos tipos de comportamiento deben ser igualmente sancionables en todos los Estados miembros con independencia de que sean cometidos o no a través de Internet".*

- **Provocación**

El artículo 18 CP[249], dispone:

"1º. La provocación existe cuando directamente se incita por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito. Es apología, a los efectos de este Código, la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor. La apología solo será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito.

2º. La provocación se castigará exclusivamente en los casos en que la Ley así lo prevea".

El fundamento del castigo de tales actos radica en el peligro especial que supone la implicación de otras personas en el plan delictivo, dado que los mismos tienen de común su finalidad captadora de voluntades, como sucede con el caso mencionado de la fabricación de moneda, el acto preparatorio tipificado y penado especialmente es la única forma posible de llevar a cabo la preparación del hecho materialmente lesivo y el sentido preparatorio del acto es, por ello, inequívoco la

[248] Ibídem.
[249] Ibídem.

fabricación (artículo 386.1 CP[250]), con respecto a la expedición (artículo 386.3 CP), de moneda falsa por los mismos falsificadores. Los tipos de preparación, sin embargo, pueden configurarse en torno a un determinado acto preparatorio particular entre otros posibles que a diferencia de aquél permanecen impunes.

El artículo 579[251] plantea en materia penal: "1. La provocación, la conspiración y la proposición para cometer los delitos previstos en los artículos 571 a 578 se castigarán con la pena inferior en uno o dos grados a la que corresponda, respectivamente.

Cuando no quede comprendida en el párrafo anterior o en otro precepto de este Código que establezca mayor pena, la distribución o difusión pública por cualquier medio de mensajes o consignas dirigidos a provocar, alentar o favorecer la perpetración de cualquiera de los delitos previstos en este capítulo, generando o incrementando el riesgo de su efectiva comisión, será castigada con la pena de seis meses a dos años de prisión.

2. Los responsables de los delitos previstos, sin perjuicio de las penas que correspondan con arreglo a los artículos precedentes, serán también castigados con la pena de inhabilitación absoluta por un tiempo superior entre seis y veinte años al de la duración de la pena de privación de libertad impuesta en su caso en la sentencia, atendiendo proporcionalmente a la gravedad del delito, el número de los cometidos y a las circunstancias que concurran en el delincuente.

3. A los condenados a pena grave privativa de libertad por uno o más delitos comprendidos en este Capítulo se les impondrá además la medida de libertad vigilada de cinco a diez años, y de uno a cinco años si la pena privativa de libertad fuera menos grave. No obstante lo anterior, cuando se trate de un solo delito que no sea grave cometido por un delincuente primario, el Tribunal podrá imponer o no la medida de libertad vigilada en atención a la menor peligrosidad del autor.

4. En los delitos previstos en esta sección, los jueces y tribunales, razonándolo en sentencia, podrán imponer la pena inferior en uno o dos grados a la señalada por la ley para el delito de que se trate, cuando el sujeto haya

[250] Vid. Ley Orgánica 10/1995, de 23 de noviembre, del Código penal, (1995).
[251] Ibídem.

abandonado voluntariamente sus actividades delictivas y se presente a las autoridades confesando los hechos en que haya participado, y además colabore activamente con éstas para impedir la producción del delito o coadyuve eficazmente a la obtención de pruebas decisivas para la identificación o captura de otros responsables o para impedir la actuación o el desarrollo de organizaciones o grupos terroristas a los que haya pertenecido o con los que haya colaborado".

A lo cual, GABARI[252] analiza aquellas conductas que tienden a preparar el delito y que constituyen un estadio intermedio entre la ideación criminal (pensar o fantasear con la posibilidad de delinquir) y la ejecución propiamente dicha (cuando las ideas del sujeto se manifiestan al mundo exterior), las resoluciones manifestadas sólo se castigarán cuando el Código Penal expresamente lo establezca. En estos casos se impondrá la pena inferior en uno o dos grados a la prevista para el delito de que se trate (consiste en coger el límite inferior de la pena y restarle la mitad de su cuantía, constituyendo aquél el límite máximo y ésta el nuevo límite mínimo).

El artículo que tratalas resoluciones manifestadas tales como la conspiración, la proposición, la provocación y la apologíaanaliza las modificaciones CP de la siguiente forma[253]:

El capítulo VII del Título XXII del Libro II CP[254] se completa con una segunda sección, "De los delitos de terrorismo", que siguiendo las directrices marcadas por la Decisión Marco 2008/919/JAI del Consejo de Europa, refleja siguientes modificaciones:

- Se añade un número 3 al artículo 576, ampliando de esta forma el concepto de colaboración con organización o grupo terrorista. Se incide en que "así se ofrece la oportuna respuesta punitiva a la actuación de los grupos o células, e incluso de las conductas individuales, que tienen por objeto la captación, el adoctrinamiento, el adiestramiento o la

[252] GABARI GÁMEZ, A. (2015). Ob., cit.
[253] SERVICIO DE ABOGADOS. (26 de abril de 2015). Ob., cit.
[254] Vid. Código penal, Ley Orgánica 10/1995, de 23 de noviembre, *Boletín Oficial del Estado (BOE)* 281, pp. 33987-34058.

formación de terroristas".

- Siguiendo las directrices de la Decisión Marco y el Convenio del Consejo de Europa sobre terrorismo, se recogen en el apartado primero del artículo 579 "las conductas de distribución o difusión pública, por cualquier medio, de mensajes o consignas que, sin llegar necesariamente a constituir resoluciones manifestadas de delito (esto es, provocación, conspiración o proposición para la realización de una concreta acción criminal) se han acreditado como medios innegablemente aptos para ir generando el caldo de cultivo en el que, en un instante concreto, llegue a madurar la decisión ejecutiva de delinquir"[255].

PUENTE GUERRERO (2011) cita en su libro a ECKSTEIN: Este "nos presenta dos niveles causales complementarios en la etiología del terrorismo: los precipitantes (eventos o sucesos concretos que inmediatamente preceden o disparan el comienzo del terrorismo, como provocaciones, masacres, aumento de la violencia interna, de las capacidades militares, de la actividad en los santuarios de la organización, entrenamiento y reclutamiento especial, desaparición de personas clave, etc.) y las precondiciones (base para el surgimiento del terrorismo a medio y largo plazo, que pueden ser estructurales) como ausencia de democracia, libertades civiles, justicia social, experiencias históricas de violencia política, etc., y situacionales (como el apoyo popular, expectativas de apoyo por la diáspora, éxito de grupos rivales, cobertura mediática, etc.). Estos niveles causales son específicos de los ámbitos en que se generan (mundial/internacional, regional/nacional, grupal e individual)".

En suelo europeo: "En cuanto a la Provocación a la comisión de un delito de terrorismo,los Estados miembros adoptarán las medidas necesarias para garantizar que la distribución o difusión pública, por cualquier medio, de mensajes destinados a inducir a la comisión de cualquiera de los delitos enumerados en el artículo 3, apartado 2, letras a) a h), cuando dicha conducta, independientemente

[255] Vid. 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. *BOE* Núm. 77, pp. 27177-27185.

de que preconice o no directamente la comisión de delitos de terrorismo, conlleve el riesgo de comisión de uno o varios de dichos delitos, constituya un delito punible cuando se cometa dolosamente"[256].

PUENTE GUERRERO (2011) desarrolla el constructo de Derecho Penal del enemigo enmarcándolo dentro de la "expansión secretaria"[257] caracterizada por la anticipación de la punición a fases alejadas de la comisión del delito, como la conspiración o la pertenencia a organizaciones criminales, equiparando las intervenciones a otras más próximas a la conducta lesiva o peligrosa. Asimismo, lleva aparejados un incremento de las penas de prisión, una amplia restricción de la obtención de beneficios penitenciarios, y el recurso a medidas de seguridad, tanto de aplicación previa a la condena como tras la excarcelación, así como la acumulación de penas y medidas de seguridad. Esta descripción recuerda en grado sumo a las reformas legales expuestas en este trabajo. El autor concluye que las reformas político-criminales que siguen el modelo de la seguridad ciudadana descrito buscan la efectividad a corto plazo ("barrer la delincuencia de las calles"), y vulneran la racionalidad del Derecho Penal; asevera que la búsqueda de efectividad a mediano y largo plazo pasa por abordar las causas sociales y políticas que generan las manifestaciones delictivas.

GONZÁLEZ HURTADO (2013), en su análisis del derecho penal español plantea que*éste castiga penalmente no sólo el autor material del hecho, sino también otros modos de autoría y participación. El artículo 27 CP establece que son penalmente responsables los autores y los cómplices, y a continuación en el artículo 28 CP se establece la posibilidad de la autoría mediata y la coautoría, así*

[256] Vid.EUROPEAN COMMISSION. (2015). Ob., cit.

[257] En este sentido, BERNARDO DEL ROSAL BLASCO, citando a THOMÉ, indica que la noción de seguridad ciudadana comprende tres dimensiones: la objetiva, conectada a la probabilidad estadística de ser víctima de un delito; la subjetiva, vinculada al miedo al delito, es decir, a la percepción del riesgo de sufrir un delito por parte de los individuos; en tercer y último lugar, se encuentra la dimensión de seguridad ciudadana tolerable, cuestión de índole cultural, ideológica o incluso política, conectada con el umbral más alto o más bajo de aceptación de los riesgos. El autor asevera que es la dimensión subjetiva la que determina la tolerancia e influye así en las demandas de seguridad y en las actitudes frente al delito y las instituciones. Por ello, apunta que la seguridad ciudadana no se asocia con la delincuencia, sino con la cohesión, solidaridad y certidumbre, de modo que se genera por el debilitamiento de las relaciones y los compromisos entre las personas. Afirma que el mayor reto que tiene la seguridad es el fortalecimiento de los vínculos de la comunidad en una sociedad con tendencia a su aplanamiento, concluyendo que no es el delincuente quien crea problemas sociales, sino que los problemas sociales son los que crean delincuentes. BERNARDO DEL ROSAL BLASCO. "¿Hacia el Derecho?", cit., p. 21.

como de otras formas de intervención como la inducción y la cooperación necesaria. El artículo 61 CP establece la misma pena a efectos sancionadores para los autores, inductores y cooperadores necesarios, y la inferior en grado para los cómplices. El tipo del artículo 264 CP no tiene especiales complicaciones en estos puntos, deberán ser los tribunales los que determinen en cada caso cual es la posición que ocupan los sujetos que han intervenido en el delito, siendo quizá está la forma de castigar penalmente a creadores o divulgadores de virus informáticos o software malicioso, no tanto por esa acción en sí, sino como por su labor necesaria al crear dichos programas para la ejecución posterior de los daños informáticos, como una suerte de cooperadores necesarios.

Por último, la autoría mediata en este tipo de delitos es perfectamente apreciable y, en muchas ocasiones, puede ser la forma habitual de realización de los hechos. Piénsese en una situación en la que un sujeto envía un virus informático a un ordenador, en el que no se produce ningún daño hasta que el usuario de ese sistema informático realiza una acción determinada (método de acción de las bombas lógicas). Esta situación no lleva al usuario que ha realizado la acción a la posición de sujeto activo, muy al contrario, dicho usuario, aun siendo el autor material del hecho, ha actuado sin libertad ni conocimiento de la situación, circunstancia que sabía el autor mediato para favorecerse y producir el daño.

Más interesante puede resultar conocer cuándo se produce la acción típica del autor mediato, si en el momento en que él completa la acción que se le presupone como autor mediato, o si ésta no se produce hasta que el autor inmediato efectivamente realiza la acción típica. La especial naturaleza de estos delitos recomienda no dar por absoluta una hipótesis, por lo que parece la solución más prudente esperar a conocer exactamente los hechos concretos y la participación exacta de cada parte en este tipo de casos.

Hay que tener en cuenta que, al ser la pena prevista inferior a 2 años de prisión, es improbable que el condenado por este delito ingrese efectivamente en ella si carece de antecedentes penales. En cuanto a las prohibiciones a las que se refiere la última parte del artículo, son las llamadas 'penas accesorias', para las

que el mencionado artículo 57[258] se remite a su vez al artículo 48[259]. Según éste, son cuatro medidas las que puede adoptar:

- La privación del derecho a residir en determinados lugares o acudir a ellos (por ejemplo, donde residan la víctima o sus familiares).
- La prohibición de aproximarse a la víctima, o a aquellos de sus familiares u otras personas que determine el juez (incluyendo a su domicilio, a sus lugares de trabajo y a cualquier otro lugar que sea frecuentado por ellos).
- La prohibición de comunicarse con la víctima, o con aquellos de sus familiares u otras personas que determine el juez (impide al penado establecer contacto escrito, verbal o visual con ellas por cualquier medio de comunicación o medio informático o telemático).
- El juez o tribunal podrá acordar que el control de estas medidas se realice a través de aquellos medios electrónicos que lo permitan.

CASTAÑÓN ÁLVAREZ (2012), comenta que en la Decisión Marco 2008/919 en su artículo 1 se entiende por provocación a la comisión de un delito de terrorismo "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) (de la Decisión Marco 2002/745 JAI), 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".

Este nuevo párrafo recoge un acto preparatorio subsidiario o residual para el supuesto de que la conducta no reúna los requisitos de la conspiración, proposición o provocación, expuestos en el párrafo anterior del mismo artículo, o en otros preceptos CP. La nueva modalidad delictiva exige, por una parte, que el sujeto activo tenga la intención de provocar, alentar o favorecer la perpetración del delito, y por otra, que con su conducta se genere o incremente el riesgo de la efectiva comisión de un delito de terrorismo. A primera vista, se trata de una

[258] Vid. 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. *BOE* Núm. 77, Artículo 57.

[259] Ibídem.

especie de fórmula cajón de sastre indeterminada y laxa, que puede llegar a castigar conductas tales como la mera adhesión ideológica al programa político de una organización terrorista; no es ni una provocación (en el sentido de incitación directa), ni una apología (provocación indirecta, ensalzamiento del crimen o enaltecimiento de su autor); además, respecto a este último, resulta curioso que, aun suponiendo la nueva conducta tipificada ahora, una infracción de menor gravedad que el propio delito de apología, sin embargo, exige un mayor contenido de injusto (incrementar el riesgo de comisión de delitos de terrorismo), algo totalmente incomprensible. A primera vista, podría parecer que la razón que justifica la incorporación de este nuevo párrafo, es la de responder a la necesidad de transcribir el concepto de provocación a la comisión de un delito de terrorismo que prevé el artículo 1.1 de la Decisión Marco 2008/919/JAI, de 28 de noviembre. Ahora bien, este artículo 1.1, sólo obliga a tipificar la provocación a los delitos de terrorismo, entendiendo por tal, "la incitación directa a la comisión de los mismos, con el consiguiente riesgo aludido", comportamiento éste que ya estaba tipificado en el Código Penal y que es diferente al que ahora ha incluido la nueva reforma: una cosa es inducir y otra alentar o favorecer. Se puede decir que el nuevo párrafo recoge dos conductas diferentes:

1- Provocación de los delitos de terrorismo que genere o incremente el riesgo de su efectiva lesión.
2- Alentar y favorecer delitos de terrorismo generando o incrementando el riesgo de su efectiva lesión.

En cuanto a la primera modalidad, la provocación, es una reiteración innecesaria de la conducta descrita en el primer párrafo del mismo artículo, entendiendo provocación como tentativa de inducción, y perpetración, como ejecución efectiva. En ambos casos, (provocación del apartado primero y provocación del párrafo segundo) los requisitos exigidos para ambas conductas son idénticos. En ambos casos, el sujeto activo con su conducta, ha de incitar expresamente y motivar al grupo indeterminado de destinatarios a la comisión de un delito de terrorismo; además, deberá comprobarse que su intención era generar en ese grupo indeterminado de destinatarios la resolución de consumar esos delitos.

En cuanto a la conducta de "alentar y favorecer la perpetración de los delitos de terrorismo, generando o incrementando el riesgo de su efectiva lesión", no responde a lo dispuesto en la Decisión Marco de 2008, puesto que como ya se ha mencionado anteriormente, en ella sólo se recomienda la sanción de la provocación, no el favorecimiento. Ya existían preceptos en nuestro Código Penal que sancionaban este tipo de conductas de favorecimiento, apoyo, etc. por ejemplo el artículo 170.2 CP, donde se contempla una conducta de incitación indirecta, o el artículo 578, que se puede decir que abarca todo tipo de elogio, alabanza o legitimación de los delitos de terrorismo, que exige además un elemento de incitación al delito, absorbiendo de esta manera las conductas de favorecimiento del párrafo segundo del apartado 1º del artículo 579 CP.

Para ALONSO GARCÍA (2015), la provocación existe cuando directamente se incita por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito. De ello se deduce que, efectivamente, las redes sociales aparecen como medio idóneo para la comisión de este tipo delictivo, al constituir "cualquier otro medio de eficacia semejante, que facilite la publicidad". La polémica en torno a este delito es de gran interés debido a determinados acontecimientos, entre los que hay que destacar el asesinato de la Presidenta de la Diputación de León, ISABEL CARRASCO. En este sentido, un joven de León de 20 años fue imputado tras publicar en su cuenta de twitter algunos comentarios ofensivos en los que pide la muerte de varios políticos y cargos públicos. Dichos comentarios rezaban así: "solo espero que ISABEL CARRASCO sea la primera de muchos más que mueran tiroteados", "lo único que me da pena de ISABEL CARRASCO, es que no pusieran una bomba y matasen a 30 o 40 politicuchos más".

III.2.6.- Humillación a las víctimas

Como precedente podemos ver que en enero del año 2015, FACU DÍAZ, guionista y director del programa de televisión '*Tuerka News'*, fue imputado por el juez de la Audiencia Nacional JAVIER GÓMEZ BERMÚDEZ por la emisión de un 'sketch' en el que establecía un paralelismo entre el PP y ETA, a instancia de una denuncia de la asociación Dignidad y Justicia.

En aquella ocasión el juez BERMÚDEZ archivó la causa, declarando en su auto que "sin hacer juicios valorativos sobre el buen o mal gusto de la escenografía usada o sobre el uso de algo tan terrible como el terrorismo para hacer un espacio de humor", el '*sketch*' no suponía" descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares"[260].

"En el Título XXII del Libro II CP («Delitos contra el orden público»), encontramos el Capítulo VII («De las organizaciones y grupos terroristas y de los delitos de terrorismo»), cuya Sección 2ª trata de los delitos de terrorismo (artículos 572 a 580 del CP). En dicha sección se enmarca el artículo 578 del CP, que en su punto 1 contempla dos tipos de conductas, de las cuales la primera está constituida por los actos de enaltecimiento o justificación públicos del terrorismo o de sus ejecutores y la segunda está constituida por los actos de descrédito, menosprecio o humillación de las víctimas del terrorismo o de sus familiares; los puntos 2 a 5 establecen diversas previsiones, en especial cuando la comisión sea a través de las Tecnologías de Información y Comunicación TIC (incremento de penas, retirada de contenidos, supresión de enlaces, etc.). El artículo 579 castiga las «resoluciones manifestadas» (conspiración, provocación y proposición), incluyendo la incitación pública indirecta a la comisión de delitos terroristas mediante difusión de mensajes o consignas y la incitación pública directa o la solicitud privada de comisión de delitos terrorista, y dispone la posibilidad de adoptar las medidas establecidas en los puntos 4 y 5 del artículo anterior. El artículo 579 bis contempla la imposición añadida de determinadas penas de inhabilitación y de la medida de libertad vigilada (puntos 1 y 2), la imposición de pena inferior por abandono de la actividad delictiva, confesión y colaboración con las autoridades o menor gravedad del hecho (punto 3). Por último, el artículo 580 dispone la equiparación de las sentencias condenatorias dictadas por jueces o tribunales extranjeros por delitos de terrorismo, a las dictadas por jueces y tribunales españoles, a efectos de reincidencia. En el Código Penal, como se observa, se regulan de forma específica los delitos de enaltecimiento o justificación del terrorismo o de sus ejecutores, o de descrédito, menosprecio o humillación de

[260] EUROPA PRESS. (26 de junio de 2015). ¿Cómo castiga el Código Penal la humillación a las víctimas del terrorismo? Recuperado de http://www.europapress.es/nacional/noticia-castiga-codigo-penal-humillacion-victimas-terrorismo-20150624174852.html

las víctimas del terrorismo o de sus familiares, cometidos a través del medio digital, de modo que resultan de aplicación los específicos puntos del artículo 578 del CP, el cual, junto con los preceptos que le siguen en la Sección 2ª, se transcribe a continuación, sin perjuicio de la aplicación, en caso de perpetración por menores, de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

La Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP, en materia de delitos de terrorismo (vigente a partir del 1/7/2015), reelabora y amplía el texto del precepto, cuya versión anterior era la siguiente:

El enaltecimiento o la justificación por cualquier medio de expresión pública o difusión de los delitos comprendidos en los artículos 571 a 577 de este Código o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares se castigará con la pena de prisión de uno a dos años. El Juez también podrá acordar en la sentencia, durante el período de tiempo que el mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57 de este Código" (ALONSO GARCÍA, 2015).

¿Cómo castiga el Código Penal la humillación a las víctimas del terrorismo? ¿También tenemos la vía civil?

Responsabilidad civil *ex delito.*

La existencia de casos en que el delito no se perpetra sobre víctimas determinadas, explica que las sentencias recaídas en los mismos carezcan de pronunciamiento al respecto. Sin embargo, cuando el delito se perpetra respecto a víctimas determinadas, se puede reclamar la responsabilidad civil que pueda corresponder, interesando, para el caso de que finalmente se estime la existencia de infracción penal, la indemnización que resulte procedente, por daños y por perjuicios morales (por la afrenta, desasosiego y, en definitiva, sufrimiento psicológico, producidos por los hechos objeto de denuncia). En este sentido, resulta conveniente aportar informe pericial psicológico o solicitar exploración pericial psicológica forense para acreditar la entidad de la afectación emocional o

psíquica sufrida por la víctima; en el caso de los menores, debe tenerse igualmente en cuenta la extensión de la responsabilidad civil a otras personas responsables.

Aunque es frecuente observar sentencias en las que no se acuerda dicha responsabilidad, en muchas ocasiones es porque la misma no se solicita. En este sentido, puede citarse la Sentencia de la Audiencia Nacional (SAN) de 29-02-12, antes referenciada, que condenó por delito de humillación a víctimas del terrorismo, a un individuo que tras acceder al perfil de la emisora «Hala Bedi» en la red social *Facebook* y localizar a través del navegador Google una noticia publicada en ABC sobre el desacuerdo de una eurodiputada con la decisión del Servicio Andaluz de Salud de financiar la fertilización de una mujer condenada por acciones terroristas, visitó la página web de la citada eurodiputada y a través del formulario de contacto envió un mensaje tipo *post* con el texto «A ver si con un poco de suerte te pegan un tiro antes de la tregua definitiva y así te reúnes con "los tuyos", so zorra... un besito», accediendo seguidamente a la sección de dicha página dedicada al hermano de la eurodiputada asesinado junto a su esposa por la organización terrorista ETA. El post remitido a la página web de la eurodiputada fue conocido por los dos colaboradores de la misma en el Parlamento Europeo al consultar el correo oficial con el que está asociada la página, imprimiéndolo y comunicándoselo a ésta al acudir a su despacho. El tribunal, haciendo referencia a la imposibilidad de establecer una indemnización a favor de la víctima por no haberse solicitado, señala: "Careciendo la acusación popular de la necesaria legitimación al efecto y no ejerciéndose por el Ministerio Fiscal acción civil, no procede establecer indemnización alguna a favor de Dña. MARÍA DEL PILAR"[261] (ALONSO GARCÍA, 2015).

La violencia en internet afecta todos los días a miles de niños, adolescentes, jóvenes y no tan jóvenes, que acceden a Internet.Muchos buscan refugio en la diversidad que proporciona la web, y algunos encuentran consuelo en libros, blogs, música y más, pues su mayor dificultad es socializar con la gente cara a cara. Y es que esta herramienta oculta no sólo a la persona en corporeidad, sino que deja reconstruir a voluntad a cualquier individuo en imagen, forma y hasta personalidad. Cualquier persona en la red puede ocultar su físico y también mentir respecto a su

[261] Vid. Sentencia nº. 11/2012, de 29 de febrero [ARP 2012, 1026].

género, edad, ocupación, nacionalidad, etcétera, permitiéndole diseñarse virtualmente, por ejemplo para difundir mensajes que justifican la anorexia o la bulimia. Esta posibilidad puede resultar muy atractiva para algunas personas, pero también muy peligrosa para otras (TRUJANO RUIZ, DORANTES SEGURA, & TOVILLA QUESADA, 2009).

En estas páginas, el escudo principal una vez más es la libertad de expresión expuesta en Internet, en donde se incita o se reprime el hecho de demostrar que hay una enfermedad de por medio. Aunque se continúan cancelando algunas de sus páginas, debido a los tipos de violencia que incluyen en sus guías de "supervivencia" y a las amenazas, insultos, humillaciones, desprecios y desvalorizaciones que contienen, además de las invitaciones a unirse a los grupos de ANAS y MIAS[262]; lo cierto es que las principales páginas siguen accesibles a cualquier usuario, sin contar con que cada día aparecen nuevas (TRUJANO RUIZ et al, 2009).

Es un hecho que nuestro mundo se diversifica cuando utilizamos la tecnología de Internet. Y es que en el ciberespacio podemos hablar, intercambiar ideas y asumir personalidades de nuestra propia creación; además, tenemos oportunidad de construir nuevos tipos de comunidades, en las que participamos con gente de todo el mundo; gente con la que podemos intimar, pero con la que quizá nunca nos reunamos físicamente.

Por otro lado, el *cyberbulling* (acoso virtual) ha sido definido como la conducta repetitiva de acercarse para amenazar a una persona por medio de las herramientas de Internet; es decir, mails, chats, tableros de foros, blogs, mensajes instantáneos, etcétera, u otros instrumentos electrónicos de comunicación, con el fin de ridiculizar o atemorizar a cientos de conocidos y desconocidos. En algunos casos, este tipo de acoso rebasa los límites de la vida real, ya que el lenguaje utilizado suele ser mucho más fuerte en los espacios virtuales, y la estrategia del acosador comprende hacer pública la información adquirida o inventada de la víctima, pues es posible adjuntar materiales ofensivos, pornográficos o personales, que dañen su integridad psicológica.

[262] Webs que fomentan la anorexia.

Cabe señalar que los efectos secundarios de este tipo de páginas pueden incluir el desarrollo de estrés y ansiedad, así como sentimientos de humillación, ira, impotencia y fatiga; y aunque en pocos casos se ha notificado la presencia de enfermedades físicas, en gran parte de estas situaciones el individuo que está siendo acosado llega a sufrir una enorme pérdida de confianza en sí mismo. "Mucho más allá de los acosos, existe el mito de la violencia extrema; es decir, el *snuff*, también denominado *white heat* o the *real thing*, y son películas en donde la víctima es filmada mientras se le golpea, tortura, viola o asesina, con el único fin de registrar los hechos, como si se tratase de una diversión. El snuff ha sido el protagonista de diferentes historias que intentan encontrar la verdad oculta en las líneas del Internet, porque el debate de su existencia se ha vinculado a redes pedófilas y a ritos satánicos o heréticos. Páginas como youtube.com y killsometime.com, favorecen la industria violenta. Es claro que esta nueva era tecnológica cambia el modo de construir la realidad y aloja a los personajes más increíbles.

Ciertamente, la violencia que atañe a nivel individual en la red podría parecer exagerada e incierta. Pero debemos considerar que la información, fotos y datos personales que miles de personas ponen a disposición de conocidos y desconocidos *en spaces, blogs* y *chats*, entre otros, los colocan en un grave riesgo, debido a que proporcionan voluntariamente su nombre, gustos, preferencia sexual, fotos, diarios y más, mismos que pueden ser manejados para violentarlos; esta información, además, ha sido utilizada para obstaculizar el ingreso de las víctimas a centros educativos, laborales y hasta religiosos.

Para FERRERES MUÑOZ (2016), el ciberbullying no es más que una ampliación del *bullying* tradicional, pues se usan las TIC para llevarlo a cabo por una serie de beneficios que éstas ofrecen, por lo que las nuevas políticas tienen que ir entorno, no solo del desarrollo del acoso en su espacio físico, sino también orientado hacia los espacios virtuales e inmateriales. El elemento esencial para que nos encontremos ante una situación de acoso es la reiteración o repetición de las conductas de hostigamiento, humillación o cualquier otra similar entre iguales, a lo largo del tiempo, de menor a mayor entidad. Una de las características que el ciberbullying tiene, y que le diferencia del bullying tradicional, es que las víctimas no pueden huir del agresor, ya que en cualquier sitio o en cualquier momento

puede mantener contacto el agresor con ésta. Y, además, mantiene el anonimato, factor muy importante a tener en cuenta, el cual será tratado en los siguientes apartados.

"Resulta importante hacer referencia al concepto de violencia porque la mayoría de conductas que llevan a cabo los menores contra sus iguales son violentas. Ésta se trata de la aplicación de la fuerza física o psíquica para obligar a otro a realizar lo que no quiere, una forma fácil pero negativa de vencer las resistencias puestas por los demás"[263] . Y lo que es importante, ésta tiene lugar en los intercambios entre los individuos. Está muy integrada en las culturas y en la sociedad en general, llegando algunos tipos de violencia a ser incontrolables. La violencia está siendo integrada por los individuos como algo bueno, que les puede ayudar a conseguir sus propios objetivos. Quizás sea esto el resultado de una cultura individualista, que promueve la competencia más que la cooperación entre los seres humanos. Las personas son seres dependientes del resto.Se necesita al resto de individuos para poder avanzar.

Existen muchos tipos de violencia y se puede ejercer de muchas otras formas. Pero en este caso, se trata la violencia a través de las nuevas tecnologías de la información y la comunicación. Esta violencia es transferida a los menores, quienes tampoco se abstienen de llevarla a cabo. De esta manera, los menores han aplicado el uso de las TIC (que en principio es algo innovador y positivo) para facilitar una conducta que mucho antes ya se llevaba a cabo. No es algo nuevo, sino que la novedad es el medio utilizado para llevarla a cabo. Por lo tanto, no es más que la conducta de bullying que ya se viene llevando a cabo desde tiempo atrás, pero a través de las TIC. Es la alarma social que han causado muchos casos (el suicidio del menor, como, por ejemplo, en el caso de Amanda) que han motivado movilizaciones para producir un cambio y mostrar rechazo hacia estas conductas.

[263] IBERTI, J. (2001). Violencia y escuela.

III.2.7.- Difusión

El Código penal lo define así (PONTE, 2015): Art. 579.CP- DIFUSIÓN DEL MENSAJE TERRORISTA (ilustración 37).

Conducta tipificada:	Difusión de mensaje o consignas que tengan como finalidad o, por su contenido, sean idóneos para incitar a otros a la comisión de delitos de terrorismo.
Medio:	Medios públicos (comunicación, conferencia, sermón, etc.)
Pena:	Inferior en uno o dos grados al delito propuesto.
Demás actos de proposición, provocación y conspiración (difusión en privado):	Pena inferior en uno o dos grados al delito propuesto.

Ilustración 37: *Difusión mensaje terrorista.*

En el análisis de VÁZQUEZ LIÑÁN (2000) se plantea: En Internet, prácticamente cualquier grupo político, guerrillero, de oposición, etc., puede tener una plataforma para expresar su versión de los hechos: también en la guerra. Mientras algunos profesionales de la información discuten sobre el sexo de los ángeles, el G-8 se reunió en París en mayo de 2000 para tratar de la seguridad en la Red, en aspectos tan clave como el ciberterrorismo. Una de las preguntas con las que el ministro japonés de Relaciones Exteriores, YOHEI KONO, abrió su discurso en este foro fue la siguiente: "¿Los hackers podrían matar a través de la red el día de mañana?".

Esta pregunta, formulada deliberadamente de una forma tan sensacionalista, coloca de inmediato al tema de fondo al nivel de importancia que se merece. Hoy día se pueden destruir industrias con sólo apretar un botón, piratear sistemas de control aéreo, atacar los sistemas informáticos de una central nuclear, etc. Países como Estados Unidos, cuyas bases de datos y sistemas de seguridad están siendo bombardeados (el vocabulario bélico se emplea también en este campo, y no es casualidad) por miles de hackers de todo el mundo, gastan astronómicas cifras en seguridad. Los daños del ciberterrorismo causan pérdidas de muchos millones de dólares y hay que defenderse. Definitivamente, es la guerra... en Internet. Y toda guerra implica necesariamente propaganda. En este escenario bélico que estamos dibujando no faltan los ejércitos: «El último protagonista conocido de una posible ciberguerra es el ataque de DoS (*Denial of Service* o denegación de servicio). El concepto es tan simple como temible: un

hacker accede de forma ilícita a una serie de ordenadores repartidos por el mundo e introduce en ellos las instrucciones necesarias para que a la misma hora del mismo día envíen a la vez solicitudes de servicio o información a un determinado servidor que, ante la imposibilidad de atender todas, acaba por colapsarse». El colapso de ciertos servidores en un país determinado puede, llegado el caso, colapsar el acceso a la Red de éste, produciendo el bloqueo económico con la crisis que esto lleva consigo. Desde luego, esto debe ser un «ataque organizado y en masa, a través de un ejército de hackers». Estamos hablando de estrategia militar, ni más ni menos.

La guerra ya de por sí tiene sus propias reglas, se ha llegado a ella por una serie de factores, ya sean históricos, políticos, económicos o, como suele ocurrir, una mezcla de todos ellos. A lo largo de la Historia, la propaganda bélica ha ido adoptando diferentes formatos, y adaptándose a los nuevos tiempos. La palabra hablada y escrita, la imagen, la música, etc. han sido usadas como propaganda a través de diferentes medios de comunicación (prensa, radio, cine, TV, espectáculos de masas, himnos, etc.). A esta larga lista de soportes propagandísticos hay que añadir, como no podía ser de otra forma, Internet (VÁZQUEZ LIÑÁN, 2000).

Delitos informáticos según establece la Unión Europea

En la actualidad, España, como país miembro de la Unión Europea, ve sometida su actuación legislativa a la regulación que de algunas materias se impone por parte de la Unión. Aunque ésta no ha llegado a legislar en todos los extremos en los que dispone de competencia, sí ha emitido la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones denominada “creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos”, de 26 de enero de 2001, en la que establece como orientar sus políticas legislativas respecto a los delitos informáticos y qué campos son susceptibles de regulación penal (GONZÁLEZ HURTADO, 2013):

- Delitos contra la intimidad: protección contra la recogida, almacenamiento, modificación, revelación o difusión de los datos personales de usuarios de sistemas informáticos.
- Delitos relativos al contenido: no sólo referidos a la pornografía infantil, sino también a declaraciones racistas y la información que incita a la violencia o al terrorismo.
- Delitos económicos, acceso no autorizado y sabotaje: dentro de este subapartado introduce un compendio de prácticas como la piratería, el sabotaje informático y la distribución de virus, el espionaje informático y la falsificación y el fraude informáticos.
- Delitos contra la propiedad intelectual: protección jurídica de programas de ordenador y de bases de datos, violación de derechos de autor, así como persecución de programas o artilugios informáticos que ayuden a la comisión de este tipo de delitos.

El Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001, es otra de las herramientas fundamentales del Derecho internacional para la homogenización de las legislaciones penales respecto de los delitos informáticos. A continuación señalalamos cuales son las conductas que entiende deben ser tipificadas en los ordenamientos penales de los países firmantes:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: en esta categoría engloba el acceso ilícito (no autorizado) a un sistema informático (art. 2), la interceptación ilícita de transmisiones de datos entre sistemas informáticos o dentro del mismo (art. 3), los ataques a la integridad de los datos (art. 4) o los sistemas (art. 5) y el abuso de dispositivos, es decir, la producción, venta, obtención, difusión u otra puesta a disposición de dispositivos o programas informáticos adaptados para la comisión de los delitos anteriores o de contraseñas o códigos de acceso que permitan acceder a otros sistemas informáticos (art. 6).
- Delitos informáticos: dentro de esta categoría se encontraría la falsificación informática (art. 7) y el fraude informático (art. 8) en la misma línea que las clasificaciones anteriores de la OCDE y la ONU.

- Delitos relacionados con el contenido: sanciona la producción de pornografía infantil para su distribución, la oferta, la puesta a disposición, la difusión, la transmisión, la adquisición o la mera posesión en o a través de sistemas informáticos (art. 9). 4.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10), de forma similar a las clasificaciones anteriores.

Precisamente para evitar esta realidad más que frecuente en la actualidad, el Convenio de ciberdelincuencia regula, como un delito de peligro, la difusión de virus informáticos, de tal manera que no sea necesaria la producción de un resultado. La tipificación de esta conducta en nuestro Derecho penal no sólo es recomendable, sino que además es una exigencia de los acuerdos internacionales ratificados por España (GONZÁLEZ HURTADO, 2013).

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

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

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

Por otra parte si atendemos a la responsabilidad civil *ex delicto,* el hecho de que en este tipo de delito no existan víctimas individuales específicas, afectando el delito genéricamente a los valores de convivencia de la comunidad social, explica que las sentencias recaídas en casos en los que no concurren otros delitos carezcan de pronunciamiento al respecto. Se puede reclamar la responsabilidad civil que pueda corresponder, cuando concurran otros delitos cuya naturaleza lo permita, como el de humillación a víctimas concretas del terrorismo, interesando, para el caso de que finalmente se estime la existencia de infracción penal, la indemnización que resulte procedente, normalmente en concepto de daño moral (esto ya se ha estudiado en el apartado correspondiente a dicho delito específico).

Entre los casos que podemos citar como ejemplos tenemos la detención en España de una mujer mexicana, de 38 años y originaria de Monterrey, con la acusación de que enaltecía y promovía actividades terroristas.

“De acuerdo con un comunicado de la Guardia Civil de España, cuando aún vivía en México ella experimentó “un rápido proceso de conversión al Islam, adoptando desde el principio una visión rigorista de dicha religión”.

En 2010, “todavía en su ciudad natal, dejó constancia de su profundo rechazo a su pasado católico y de su deseo de vincularse emocionalmente con un musulmán”.

En España se casó con un hombre, que a la postre sería detenido, en mayo de 2016, y que era “integrante de una red de captación y adoctrinamiento terrorista”.

Al ocurrir esa detención, según la Guardia Civil, se agudizó el "proceso de autoradicalización" de la mujer mejicana, aislándose de la comunidad en Madrid.

Con total ausencia de relaciones sociales ajenas al ámbito radical, limitando al máximo sus salidas del domicilio, siempre vistiendo el niqab y con una atención escrupulosa a las directrices del islam más radical, para diferenciar entre las conductas permitidas (halal) y las prohibidas (haram), indicó el comunicado respecto a su comportamiento.

Las indagatorias, según las autoridades españolas, llevaron a establecer que la mujer detenida ejercía una clara influencia sobre un amplio grupo de contactos, a los que incitaba a ejercer una labor proselitista.

En este sentido, llegó a erigirse en figura muy relevante entre las mujeres de la Comunidad Islámica de su tierra natal, alentando a la yihad femenina y compartiendo material propagandístico, búsquedas realizadas en Google de México y acceso a perfiles de Facebook de musulmanes conversos originarios de Hispanoamérica, apuntó la Guardia Civil.

La investigación ha podido determinar la existencia de una estructura estable que desarrollaba una intensa labor de publicación y distribución de contenidos propagandísticos afines al terrorismo yihadista, a través de diversas plataformas web y aplicaciones de mensajería instantánea, desde las que realizaban llamamientos expresos a la participación en actividades terroristas"[264].

En el ámbito digital, como ya se ha indicado anteriormente en esta obra, las plataformas de redes sociales albergan diversos cauces que permiten la perpetración de este delito, dados los variados sistemas de comunicación interna y publicación de contenidos que dichas plataformas ofrecen. En efecto, el registro como usuario en una plataforma de red social permite acceder a una gran variedad de aplicaciones informáticas de comunicación y difusión de contenidos, de utilización sencilla y normalmente gratuita, tales como el sistema de publicación de contenidos (tweets, posts), los sistemas de conversación instantánea (chats),

[264] ANIMAL POLÍTICO. (23 de enero de 2017). Redacción. Detienen en España a una mexicana por el delito de enaltecimiento y promoción del terrorismo. Periódico digital animalpolitico.com Recuperado de:http://www.animalpolitico.com/2017/01/detienen-espana-mexicana-la-acusan-difundir-propaganda-terrorista/

los sistemas de mensajería interna (e-mails), etc., lo que, sumado a los diversos sistemas de comunicación y de publicación de contenidos que en general ofrece Internet, explica la incidencia que en el medio digital presentan este delito y otras infracciones. Por otra parte, debe tenerse en cuenta que los concretos aspectos del funcionamiento técnico de las diversas plataformas de redes sociales (apertura de cuentas, acceso a la zona operativa de los perfiles, envío de comunicaciones, etc.) y otras plataformas asimiladas como los foros participativos (registro, acceso, envío de comunicaciones, etc.), pueden tener especial incidencia en la credibilidad de las manifestaciones de las partes u otros aspectos (validez de pruebas, concurrencia de requisitos materiales o procesales, etc.) y resultar determinantes en relación con el signo del pronunciamiento que finalmente se adopte, tratándose de una cuestión sobre la que acusación y defensa no pueden pasar de soslayo, pues precisamente de la misma puede derivarse la condena o la absolución. En este sentido, puede citarse la SAN de 12-7-13, que condenó por delito de difusión del terrorismo del artículo 579. 1., párrafo segundo del CP, a un individuo que procedió a colocar varios post en un foro de Internet, incitando a cometer atentados contra Occidente. El tribunal señala: "El acusado, PRUDENCIO mantenía y ha mantenido con posterioridad al 12 de julio de 2011 una intensa actividad como usuario en foros yihadistas radicales que operan en Internet, en concreto en los denominados *Al Shumukh Al Islam*, *Ansar Al Mujahideen* y *Al fidaa*, en los que albergaba con frecuencia posts, en línea y contenido con los que son frecuentes dichos foros radicales. Tanto en el foro "*Al Shumukh Al Islam*", como "*Ansar Al Mujahideen*" se difunden con frecuencia comunicados y videos elaborados por organizaciones terroristas de carácter yihadista, o relacionados con actividades violento-terroristas realizadas por estas organizaciones. Son igualmente empleados con frecuencia como medio, no sólo difusión de ideas o consignas, también para el adoctrinamiento, mútuo reforzamiento y autoafirmación de planteamientos radicales yihadistas de sus usuarios, y en ocasiones de plataforma para la captación y reclutamiento de personas interesadas en la comisión de hechos delictivos de carácter terrorista. El encausado, entraba en dichos foros utilizando como nombre de usuario el de "Farsante" y una clave, sin que exista absoluta constancia de que esta identidad virtual o *nickname* fuera utilizada únicamente por él con anterioridad al 12 de julio de 2011, que es a partir de cuándo se tiene plena constancia de su utilización por el acusado, como consecuencia de

la monitorización de su línea ADSL, con autorización judicial, por parte de la policía. Los atributos que tenía concedidos y con los que firmaba el usuario "Farsante" en el foro eran los de "shamikh el incitador" y alumno de la facultad de aprendizaje de Shumkh al Islam. (…) El Tribunal ha descartado por razones probatorias la pertenencia o integración del acusado en organización o grupo terrorista, al considerar no acreditada ésta en relación con un grupo u organización, en la forma en cómo se describen en los art 570 bis y ter del CP, en concreto; sin que aparte del *post* del 28/05/2011, que se le atribuye al acusado, al que ya nos hemos referido, exista algún otro elemento de conexión que permita vincularlo con la organización terrorista AQMI o con alguno de sus miembros o colabore de alguna forma con dicha organización. Sin embargo, el Tribunal si considera que los hechos que se tienen expresamente por probados constituyen un delito de difusión del terrorismo del art 579.1., párrafo segundo. Los hechos a los que nos referimos consisten, en síntesis, en la participación activa, profusa y reiterada en foros con los contenidos más radicales yihadistas y la administración de una página web en la que se cuelgan y se hacen disponibles para su descarga noticias, videos, etc., del mismo contenido; acciones a través de los que se induce indirectamente al terrorismo; es decir, a través de la que se provocan de forma genérica o se alientan o favorecen la realización de actividades terroristas, lo que sin duda genera un objetivo incremento de riesgo de efectiva comisión de hechos de esta clase. La naturaleza y contenido de las conversaciones mantenidas, de los post atribuibles al acusado, su propia posición en el foro, claramente son las de un firme partidario de la violencia terrorista en favor de la yihad universal, con una intención clara de generar, apoyar y alentar este sentimiento en otras personas relacionadas con el foro. Sin embargo, esta calificación no es compatible con la que también hizo el Ministerio Fiscal en la calificación definitiva de los hechos, como una de las modalidades de enaltecimiento del terrorismo del art. 578CP, que también se refiere a la difusión de los delitos de terrorismo, ya que en realidad son tipos penales alternativos, que castigan las mismas o similares conductas y que por ello no se pueden aplicar conjuntamente, en relación a una misma conducta, sin que ello no signifique un *bis in ídem*, al venirse a castigar lo mismo y por las mismas razones[265] (ALONSO GARCÍA, 2015).

[265] Vid. Sentencia nº. 24/2013 de 12 julio. JUR 2013\276501.

La reforma CP de la L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, CP (BOE 31 marzo), ha hecho muchísimo hincapié en este punto, en la línea de frenar el terrorismo en su base, intentando legislar sobre los delitos de difusión y de esta forma intentar cortarlo de raíz ya que los medios actuales de internet son tan potentes que de no ser así nos abrumarían.

III.3.- LEY 10/2010 DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO

Tal como hemos visto en puntos anteriores, a lo largo de los últimos años, el terrorismo ha golpeado a las naciones y estas se han movilizado poniendo en funcionamiento un conjunto de instrumentos y medios para contrarrestar estos ataques e intentar evitarlos.

Todas las naciones y sus efectivos coinciden que la mejor forma de combatirlos es la prevención y por supuesto el pilar más importante de la prevención es destruir su financiación. Si logran hacer flaquear su financiación lograrán evitar un porcentaje muy alto de acciones terroristas y por supuesto las de mayor calibre.

Para todo esto cada país se ha organizado y se ha movilizado para poner en marcha tanto medios jurídicos (Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo)[266], como medios operativos, todos los necesarios para aplicar dicha ley y debilitar de esta forma las estructuras de financiación del terrorismo, lo cual a su vez minimiza tanto el número como el tamaño de las acciones destructivas que los terroristas planean realizar.

III.3.1.- Estudio y fundamentación

La política de prevención del blanqueo de capitales surge a finales de la década de 1980 como reacción a la creciente preocupación que planteaba la criminalidad

[266] Vid. Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado (BOE-A-2010-6737)*, nº. 103, pp. 37458 a 37499).

financiera derivada del tráfico de drogas.

Sin embargo, debe subrayarse que la Directiva 2005/60/CE o Tercera Directiva, que básicamente incorpora al derecho comunitario las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) tras su revisión en 2003, se limita a establecer un marco general que ha de ser, no sólo transpuesto, sino completado por los Estados miembros, dando lugar a normas nacionales notablemente más extensas y detalladas, lo que supone que la Directiva no establece un marco integral de prevención del blanqueo de capitales y de la financiación del terrorismo que sea susceptible de ser aplicado por los sujetos obligados sin ulteriores especificaciones por parte del legislador nacional. Por otra parte, la Tercera Directiva es una norma de mínimos, como señala de forma rotunda su artículo 5, que ha de ser reforzada o extendida atendiendo a los concretos riesgos existentes en cada Estado miembro, lo que justifica que la presente Ley contenga, al igual que la vigente Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, algunas disposiciones más rigurosas que la Directiva[267]:

(1)"Los flujos masivos de dinero negro pueden dañar la estabilidad y la reputación del sector financiero y poner en peligro el mercado único, y el terrorismo sacude los cimientos mismos de nuestra sociedad. Unida al planteamiento basado en el Derecho penal, una actuación preventiva a través del sistema financiero puede surtir resultados.

(2) La solidez, integridad y estabilidad de las entidades financieras y de crédito, así como la confianza en el sistema financiero en su conjunto, podrían verse en grave peligro debido a los esfuerzos de los delincuentes y sus cómplices, ya sea por encubrir el origen de los productos del delito, ya por canalizar el producto de actividades legítimas o ilegítimas a fines terroristas. A fin de evitar que los Estados miembros adopten medidas para proteger su sistema financiero que puedan ser contrarias al funcionamiento del mercado interior y a las normas del Estado de Derecho y del orden público comunitario, es necesaria una actuación comunitaria en este ámbito.

[267] Ibídem.

(3) Si no se adoptan medidas de coordinación en el ámbito comunitario, los blanqueadores de capitales y los financiadores del terrorismo podrían aprovechar la libre circulación de capitales y la libre prestación de servicios financieros que trae consigo un espacio financiero integrado para facilitar sus actividades delictivas.

Para responder a estas preocupaciones en el ámbito del blanqueo de capitales se adoptó la Directiva 91/308/CEE del Consejo, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales.

(4). La Directiva instaba a los Estados miembros a prohibir el blanqueo de capitales y obligar al sector financiero, incluidas las entidades de crédito y numerosas entidades financieras de otros tipos, a identificar a sus clientes, conservar los documentos adecuados, establecer procedimientos internos de formación del personal y vigilar el blanqueo de capitales, así como comunicar a las autoridades competentes cualquier indicio de blanqueo de capitales[268]".

En el año 2005 la situación internacional al respecto del terrorismo sumado al creciente establecimiento de libre circulación en la Unión Europea de personas y capitales por la incorporación de nuevos miembros, obliga a ésta a actualizar las medidas jurídicas en la línea de controlar los movimientos monetarios que se producen dentro de la zona, con el fin de terminar con la temida amenaza terrorista.

Reduciendo la capacidad económica de las organizaciones terroristas reducimos su capacidad de acción.

Según ÁLVAREZ y EGUIDAZU (2016), en los últimos años, otro problema de primera magnitud ha venido a sumarse a las preocupaciones de la comunidad internacional que requieren una actuación prioritaria: el terrorismo internacional. No se trata, por desgracia, de un problema nuevo, pero a partir del atentado de Nueva York del 11 de septiembre de 2001, la comunidad internacional ha tomado

[268] Vid. Diario Oficial de la Unión Europea, nº 309, Directiva 2005/60/CE del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, de 26 de octubre de 2005.

conciencia del desafío que supone el terrorismo internacional, fundamentalmente el terrorismo islamista y ha promovido iniciativas para combatirlo de forma coordinada. Al igual que en el caso del blanqueo de capitales procedentes del narcotráfico, los Gobiernos han coincidido en constatar que una forma particularmente eficaz de combatir el terrorismo internacional consiste en cegar las vías a través de las cuales se financia. Ha surgido así una normativa cuyo objetivo es la prevención de las actividades de financiación del terrorismo, paralela y en muchos casos coincidente, con la de prevención del blanqueo de capitales.

Paralela e independientemente de la vía penal, los países han seguido además un camino tendente a impedir el blanqueo desenmascarando las vías y mecanismos del mismo, identificando las operaciones de los blanqueadores.

Casi desde un principio resultó evidente que el blanqueo de capitales se desarrollaba esencialmente a través del sistema financiero. Así se constató, por ejemplo, por el GAFI ya en su informe de 1997 y así lo señalaron también el Departamento del Tesoro norteamericano, o la antes citada Directiva 91/308/CEE de la Unión Europea[269].

Son varias las razones que pueden explicar este hecho: el tamaño del mercado financiero y la complejidad de sus operaciones que lo hacen idóneo, como ningún otro sector, para las operaciones de blanqueo; la gran disparidad de las reglamentaciones nacionales financieras y bancarias; la deficiente (o prácticamente nula) supervisión bancaria en algunos países y territorios; la existencia del secreto bancario, y las posibilidades de anonimato que con frecuencia brindan algunas legislaciones nacionales; las nuevas técnicas y procedimientos bancarios que, encaminados a agilizar las operaciones y facilitar los trámites a los clientes, son abundantemente utilizadas por los blanqueadores para enmascarar sus operaciones...

[269] ÁLVAREZ PASTOR, D. y EGUIDAZU PALACIOS, F. (2006). Manual de prevención del blanqueo de capitales. Barcelona: Marcial Pons, Ediciones Jurídicas y sociales, S. A. Recuperado de: https://www.marcialpons.es/static/pdf/100788061.pdf.

III.3.2.- SEPBLAC

El SEPBLAC, es un organismo que funciona en el ámbito del Poder Ejecutivo y está adscrito al Banco de España.

El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias de España (SEPBLAC) es la Unidad de Inteligencia Financiera (UIF) de España. Esta unidad especializada está teniendo más visibilidad en los medios de comunicación por sonados casos de corrupción y blanqueo como el más reciente en relación con el Banco de Madrid, el relacionado con el ex vicepresidente del Gobierno de España y ex director gerente del Fondo Monetario Internacional (FMI), RODRIGO RATO, o la lista de 715 amnistiados fiscales que están siendo investigados por el organismo. También está de actualidad entre las empresas *FinTech*, como las del sector de *Bitcoin*, que quieren conocer su situación legal con el SEPBLAC.

Las actuaciones de la SEPBLAC están dirigidas a la prevención e impedimento de la utilización del sistema financiero, empresas o profesionales para el blanqueo de capitales**.** Este organismo es el encargado de recibir, analizar y presentar a las autoridades competentes los casos de blanqueo de dinero que se derivan de la entrega de información financiera relacionada con fondos sobre los cuales se sospecha una procedencia delictiva o de la información requerida por la legislación para contrarrestar el blanqueo de dinero.

La regulación del SEPBLAC está recogida en los artículos 45-47 de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo. Es esta misma ley la que determina los 26 tipos de sujetos obligados a cumplir con esta normativa entre los que destacan entidades de crédito; aseguradores y corredores de seguros; servicios y sociedades de inversión; intermediarios financieros; asesores fiscales; contables; jurídicos y mercantiles; transporte y empresas de loterías y juegos de azar; casinos; comerciantes de joyas; metales y piedras preciosas; notarios y registradores de propiedad; personas que ejerzan actividades de cambio de moneda; entidades de pago y de dinero electrónico, entre otras.

El SEPBLAC es el organismo en el que las personas físicas o jurídicas obligadas a cumplir con esta ley deben inscribirse, así como comunicar las operaciones con indicios de blanqueo o financiación del terrorismo que se deriven de la aplicación de su manual de prevención de blanqueo de capitales. Un manual que cada empresa deberá realizar adaptándose a sus necesidades específicas y que deberá estar a disposición del organismo. Además, deberán remitir al mismo el examen externo anual realizado por un experto externo dado de alta en el SEPBLAC.

El SEPBLAC también se encarga de recibir y procesar las solicitudes de información y colaboración de organismos y autoridades nacionales e internacionales, así como, las comunicaciones derivadas de la aplicación del régimen jurídico de movimientos de capitales y de las transacciones económicas con el exterior[270].

El Plenario del GAFI, celebrado en Busán (Corea) del 19 al 24 de junio de 2016, eligió como Presidente a JUAN MANUEL VEGA SERRANO, Director del SEPBLAC, con efectos desde el 1 de julio y un mandato de un año[271].

"El GAFI es, sin duda, el más importante organismo mundial en la lucha contra el lavado; su progresiva y persistente acción ha logrado identificar no sólo los paraísos fiscales, sino que con su actividad ha logrado la cooperación de los mismos bancos como hemos visto, a los cuales se les exige la máxima diligencia en la identificación de sus clientes (según la regla *know your customer)* y por la que deberán informar a las autoridades competentes y conservar la documentación correspondiente, obligación que se hace extensiva a notarios, registradores y contadores. Este organismo subcontinental ya está instalado en la Argentina, en donde la Ciudad de Buenos Aires como sede ejecutiva (GAFIsud) del Organismo Intergubernamental, agrupa a los países de América del Sur en la lucha contra el lavado de dinero de origen delictivo. El grupo GAFIsud se ha creado de manera semejante al Grupo de Acción Financiera Internacional (GAFI),el que

[270] ORO Y FINANZAS. (29 de abril de 2015). ¿Qué es el SEPBLAC? Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias de España. Recuperado de: www.OroyFinanzas.com

[271] SEPBLAC. (2017). Servicio ejecutivo, Comisión de prevención del blanqueo de capitales e infracciones monetarias. Recuperado de: http://www.sepblac.es/espanol/presidencia_gafi/presidencia.htm

ha diseñado el estándar internacional de antilavado más reconocido del mundo, del que también nuestro país es integrante a través de su Unidad de Información Financiera (UIF). Es de destacar que el GAFI ha emitido las famosas cuarenta recomendaciones volcadas en el Documento Consultivo, cuya versión consolidada fue publicada en junio de 2003, además de las notas explicativas y un Glosario[272]. Tanto el GAFI como el GAFIsud promueven esquemas de trabajo y consultas que comprueban la marcha del combate antilavado y la conducta de los países integrantes, como asimismo un sistema de consultas. No podemos dejar de tener presente que tanto las cuarenta recomendaciones como asimismo sus recomendaciones especiales han sido reconocidas por el Fondo Monetario Internacional y por el Banco Mundial como Normas Internacionales en materia de lucha contra el blanqueo de capitales y financiación del terrorismo"[273].

III.4.- DETECCIÓN DEL DELITO

Este punto será desarrollado de forma muy básica y poco extensa ya que no es el tema que centra nuestra investigación.

Revisaremos por un lado el software más utilizado para la detección de información delictiva y por otro el mayor sistema internacional de vigilancia líder en el sector a nivel mundial.

Destacamos que en el caso del *Carnivore* su utilización sin autorización judicial sobrepasa los límites de la legalidad.

ECHELON[274] es tan poderoso a nivel técnico como humano, y en muchas de sus actuaciones puede llegar a sobrepasar los límites de legalidad de los países

[272] FATF. (1986). The Financial Action Task Force, Grupo de Acción financiera Internacional. Recuperado de: http://www.fatf-gafi.org/

[273] CABULI, E. y JATIB, G. J. (2 de mayo de 2006). La prevención del lavado de activos y el ejercicio profesional en el mundo globalizado. Revista *La Ley*. Recuperado de: https://www.colegio-escribanos.org.ar/biblioteca/cgi-bin/ESCRI/ARTICULOS/48676.pdf

[274] Echelon es un término inglés que significa "escalón", aunque esta red también es conocida como "La Gran Oreja". Es una aplicación informática cuya plataforma de trabajo abarca un entramado de antenas, estaciones de escucha, radares y satélites, apoyados por submarinos y aviones espía, unidos todos esos elementos a través de bases terrestres, y cuyo objetivo es teóricamente, espiar las comunicaciones mundiales, para luchar contra el terrorismo internacional y el tráfico de drogas. Vid. https://www.ecured.cu/Echelon

donde actúe.

III.4.1.- Sistema global nacional de vigilancia "Sistema Carnívoro"

Carnivore (en español, carnívoro) es el nombre de un *software* usado por el FBI que está íntimamente muy ligado a ECHELON.

Este software se instala en los proveedores de acceso a Internet, y tras una petición proveniente de una instancia judicial, rastrea todo lo que un usuario hace durante su conexión a Internet. En teoría tiene capacidad para discernir comunicaciones legales de ilegales e investiga todo tipo de información.

El cómo realiza este análisis, y cuál es su infraestructura y alcance real, es algo que permanece secreto. Tiene la misma procedencia que ECHELON (EE. UU.) y pertenece a una agencia estatal (FBI), al igual que ECHELON (NSA).

Sus características más importantes son:

1. Capacidad "quirúrgica" de distinguir entre sujetos interceptados y no interceptados.

2. Capacidad de distinguir entre datos interceptables de un sujeto y datos no interceptables, basándose en los poderes concedidos por la orden judicial de intercepción.

3. *Carnivore* comparte información (al igual que ECHELON) con la industria con el fin de desarrollar estándares adecuados a los requerimientos del sistema.

4. El FBI ha pedido que se estandaricen una serie de protocolos relacionados con la intercepción en Internet. Se piden esas estandarizaciones para "obtener legalmente información importante mientras se amplía o mejora la protección de la intimidad".

5. Es posible que tenga relación con el sistema espía ECHELON o simplemente que sea una de sus partes integrantes[275].

Tal como pasa con ECHELON su total legalidad es fundamentalmente el punto de desunión con la mayoría de estados y sus constituciones, siempre y cuando sea utilizado sin una previa orden judicial, ya que, de no ser así, en la mayoría de sus funciones o actuaciones sobrepasa la línea de la legalidad y pisotea el Derecho a la intimidad y a la protección de datos.

III.4.2.- Sistema global internacional de vigilancia "Sistema ECHELON"

ECHELON se considera como la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia (Inteligencia de señales, en inglés: *Signals intelligence*, SIGINT).

Esta dirigida por UKUSA (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda). ECHELON tiene capacidad de capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos en todo el mundo. También incluye análisis automático y clasificación de las interceptaciones, intercepta más de tres mil millones de comunicaciones cada día en todo el mundo.

En principio se creó con el fin de controlar las comunicaciones militares de la Unión Soviética y sus aliados.En este momento ECHELON es utilizada también para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia político-diplomática.

Su existencia fue hecha pública en 1976, desde entonces ha empezado la pugna entre lo legal y lo ilegal de sus actuaciones.

Sus miembros son de habla inglesa y pertenecen a UKUSA.Desde la Segunda Guerra Mundial este organismo no ha dejado de investigar comunicaciones en el mundo para de esta forma guiar las actuaciones de las

[275] FBI (2017). Federal Bureau of Investigation. Terrorismo. Recuperado de: https://www.fbi.gov/investigate/terrorism

naciones en materia de espionaje a otras naciones, narcotráfico y terrorismo.

En 1994, el grupo francés *Thompson*-CSF habría perdido un contrato con Brasil por valor de 1300 millones de dólares en favor de la empresa estadounidense *Raytheon*, gracias a información comercial interceptada por ECHELON que habría sido suministrada a *Raytheon*. Ese mismo año Airbus habría perdido un contrato de 6000 millones de dólares con Arabia Saudita en favor de las empresas estadounidenses *Boeing* y *McDonnell Douglas*, gracias a que las negociaciones entre Airbus y sus interlocutores árabes habrían sido interceptadas por ECHELON y la información facilitada a las empresas de las naciones socias[276].

Esta gran organización UKUSA está dirigido por la NSA (*National Security Agency*), cuenta con más de 100.000 empleados tan sólo en Maryland (Estados Unidos) (otras fuentes hablan de 380.000 empleados a escala mundial), por lo que es con toda seguridad la mayor organización de espionaje del mundo[277].

Normalmente la información es enviada desde Menwith Hill (Reino Unido) por satélite a *Fort Meade* en Maryland (EE.UU.). Cada estado dentro de la alianza UKUSA tiene asignado una responsabilidad sobre el control de distintas áreas del planeta.

La tarea principal de Canadá solía ser el control del área meridional de la antigua Unión Soviética. Después de la guerra fría se puso mayor énfasis en el control de comunicaciones por satélite y radio en centro y Sudamérica, principalmente como medida para localizar tráfico de drogas y secuaces en la región.

Los Estados Unidos, con su gran cadena de satélites espías y puertos de escucha controlan gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China.

[276] GIBSON, W. (2004). Pattern Recognition/Mundo espejo. Versión española. Minotauro.

[277] BURBUJA. (9 de agosto de 2013). Echelon: la mayor red de espionaje del mundo. Recuperado de: https://www.burbuja.info/inmobiliaria/conspiraciones/449941-echelon-mayor-red-de-espionaje-del-mundo.html#

Gran Bretaña intercepta comunicaciones en Europa, Rusia y África; Australia examina las comunicaciones de Indochina, Indonesia y el sur de China; Nueva Zelanda barre el Pacífico occidental.

El desarrollo de estos sistemas se ha extendido por otros países, entre los que cabría destacar la creación de un centro OSINT en la universidad sueca de Lund.

Por supuesto en estas últimas décadas, siguiendo las líneas de la tecnología, estos estados han ubicado estaciones de intercepción electrónica y satélites espaciales para capturar gran parte de las comunicaciones establecidas por radio, satélite, microondas, móviles y fibra óptica. Su capacidad es de tal envergadura que probabemente sea el mayor instrumento mundial en el manejo de tecnología en informacion. Se capturan señales que posteriormente son procesadas por un conjunto de superordenadores, denominados en jerga tecnológica como *diccionarios*, que son programados concretamente para buscar patrones específicos en todas y cada una de las comunicaciones procesadas, en función de ser direcciones, palabras, frases o incluso voces específicas.

Es bien sabido que el sistema dispone de 120 o mas estaciones fijas y satélites geoestacionarios que se interrelacionan entre si.

Se estima que estos sistemas filtran el 90% o más del tráfico que se mueve en Internet. Sus antenas (de ECHELON) concretamente captan ondas electromagnéticas y las trasmiten a un lugar central para su procesamiento. Estos mensajes recogidos son aleatorios y se procesan mediante los diversos filtros, se buscan palabras clave y a partir de aquí se organiza y gestiona la información en busca de resultados encatenados de forma lógica. Este procedimiento se denomina “Control estratégico de las telecomunicaciones”.

Sus contrarios afirman que el manejo de este sistema les da tanto poder que se les va de las manos y es utilizado también para el espionaje económico e invadir la privacidad a gran escala.Nace aquí la gran disputa que lo identifica legalmente, si invade y se salta todas y cada una de las constituciones que defienden los derechos de los ciudadanos en cada uno de los países analizados que en este caso y dado su potencia abarca probablemente a toda la geografía

mundial. La red de espionaje fuera del control judicial supone una privación de la libertad individual consagrada en diferentes textos legislativos internacionales y nacionales, siendo este el motivo por el que el 21 de octubre de 2001, se organizó a través de Internet un intento de colapsar o socavar a ECHELON.

Por otra parte, ECHELON también se instala en Europa y España. El 5 de julio de 2000 el Parlamento Europeo decidió crear una comisión para investigar la red ECHELON, tras estudiar el informe titulado *Capacidades de Intercepción 2000* en el que se informaba del uso de información recolectada por la red ECHELON para fines comerciales de los países UKUSA.

El Parlamento Europeo en Acta del 5 de septiembre de 2001, emitió un informe en el que se expresa que: "*considerando que no hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial*" constató la existencia de un sistema de interceptación mundial de las comunicaciones, resultado de una cooperación entre los Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda siendo "*la finalidad del sistema la interceptación, como mínimo, de comunicaciones privadas y comerciales, y no militares"*[278].

Diversos medios de comunicación fueron testigos del apoyo del expresidente español JOSÉ MARÍA AZNAR a las estrategias desarrolladas bajo la presidencia de G.W. BUSH, que habrían posibilitado la colaboración antiterrorista de los Estados Unidos, incluyendo el acceso a la red "*Carnivore*".

"¿ECHELON contra ETA? La Red especula sobre el ofrecimiento de colaboración de EE.UU. a España de utilizar su sistema de filtrado de comunicaciones para luchar contra la banda terrorista.MADRID.- ¿Es cierto que los servicios de inteligencia están pendientes de todo lo que decimos y escribimos para buscar posibles mensajes terroristas o de espías? La red de espionaje ECHELON es uno de los mitos -o realidades- más conocidas de la Red. Negada por todos los participantes, investigada por la Comisión Europea y denunciada por los internautas. Pero... ¿qué ocurriría si ahora EE.UU. 'ofreciese' su sistema de ciberespionaje a las naciones amigas para hacerlo 'oficioso'? Esto parece ser lo

[278] PARLAMENTO EUROPEO. (2001). Acta del 5 de septiembre de 2001.

que ha ocurrido durante el viaje oficial del presidente estadounidense, GEORGE Bush, a España esta semana. En la rueda de prensa ofrecida por el ministro de Asuntos Exteriores, JOSÉP PIQUÉ, éste aseguró que Estados Unidos iba a espiar las comunicaciones de ETA para España. La conclusión sacada por el diario The Guardian y cientos de personas en los foros de Internet ha sido apabullante: verde y con asas. Eso sólo lo puede hacer Echelon.

El Gobierno no ha querido comentar nada sobre la posible utilización de ECHELON. Sólo ha dicho que se están analizando las nuevas formas de cooperación con los servicios de inteligencia estadounidenses.

De hecho, en la comparecencia, el ministro PIQUÉ evitó en todo momento utilizar la palabra ECHELON, aunque tal y como publicó EL MUNDO, fuentes del gobierno aseguraron que "la información recopilada por la CIA y por sus satélites, unido a la capacidad de EE.UU. de interceptar las comunicaciones y leer el correo electrónico, podría ayudar a mantener el grupo terrorista bajo control".

Ojos en todo el mundo

La primera pista de la existencia de una red de espionaje mundial denominada ECHELON la destapó el periodista escocés DUNCAN CAMPBELL. Llamadas de teléfono, faxes, mensajes de correo electrónico... según CAMPBELL, todo ha pasado por alguna de las 140 instalaciones de la mayor red de espionaje internacional jamás conocida. Y el periodista escocés dice tener pruebas fotográficas y documentos que apoyan sus escalofriantes teorías.

Las pruebas de la implicación de los servicios de inteligencia de Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda en el entremado eran tan evidentes que el Parlamento Europeo comenzó una investigación, que concluyó con la constatación de la existencia de ECHELON. Fueron contundentes en sus explicaciones: "no hay ninguna duda acerca de la existencia de una red mundial de intercepción de datos anglosajona" aseguraba el ponente de la comisión temporal del Parlamento Europeo, el socialista alemán GERHARD SCHMID. Que se denomine ECHELON o tenga otro nombre no tiene importancia, explicó al precisar que esto implica que otros sistemas pueden estar funcionando.

La red de escuchas lleva funcionando desde 1971, aunque como es obvio, sus capacidades de interceptación de mensajes han mejorado sustancialmente con el paso de los años[279].

Esta colaboración habría permitido la detención de algunos comandos de ETA y la detención del arsenal etarra en Sokoa en el País Vasco francés basado en el informe "Una aproximación a las tecnologías de control político" de la Fundación Omega de Mánchester y presentado en la Comisión de Libertades Públicas y Asuntos de Interior del Parlamento Europeo el 27 de enero de 1998.

La red ECHELON espió al ingeniero español, JOSÉ IGNACIO López de Arriortúa, grabando la NSA una videoconferencia entre éste y su superior de la empresa alemana Volkswagen entregando a los EE.UU. la información a la empresa estadounidense General Motors (Motivo de pregunta en el parlamento por parte de la diputada de Eusko Alkartasuna BEGOÑA LASAGABASTER).

[279] CERNUDA, O. (15 de junio de 2001). Ciberespionaje: ¿ECHELON contra ETA? *Periódico digitalnavegante.com*. Recuperado de: http://www.elmundo.es/navegante/2001/06/15/esociedad/992605466.html

CAPÍTULO IV

RESPUESTA LEGISLATIVA INTERNACIONAL

IV.1.- ESTUDIO DE LA LEGISLACIÓN INTERNACIONAL. CONVENIOS INTERNACIONALES

La misión principal de este punto es la de facilitar una visión rápida y organizada de todos y cada uno de los tratados o pactos internacionales que se han firmado en materia antiterrorista, organizados cronológica y geográficamente, proporcionando un enlace web que permita el acceso a la totalidad de su contenido para de esta forma poder estudiarlos de una forma más detallada y completa.

IV.1.1.-Instrumentos jurídicos internacionales (Naciones Unidas)

A partir de 1963 y hasta la actualidad, la comunidad internacional ha creado 19 instrumentos jurídicos internacionales con el fin de prevenir actos terroristas. Los instrumentos se elaboraron bajo tutela de Naciones Unidas y el Organismo Internacional de Energía Atómica (OIEA), siendo sus Estados Miembros los participantes.

Este es el resumen de 8 convenios, a su vez formados por 19 instrumentos jurídicos universales y enmiendas complementarias en relación con el terrorismo, organizados de la siguiente forma:

Instrumentos sobre la aviación civil

1. Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves (1963): Se aplica a los actos que afecten a la seguridad

durante el vuelo. Autoriza al comandante de la aeronave a imponer medidas razonables, incluso coercitivas, contra toda persona que le dé motivos para creer que ha cometido o está a punto de cometer un acto de esa índole, siempre que sea necesario para proteger la seguridad de la aeronave y exige que los Estados contratantes asuman la custodia de los delincuentes y devuelvan el control de la aeronave a su legítimo comandante[280].

2. Convenio para la represión del apoderamiento ilícito de aeronaves (1970): Considera delito que una persona, estando a bordo de una aeronave en vuelo, ilícitamente, mediante violencia, amenaza de violencia o cualquier otra forma de intimidación, se apodere de tal aeronave, ejerza el control de la misma o intente hacerlo. Exige que las partes en el Convenio castiguen los secuestros de aeronaves con "penas severas"; exige que las partes que hayan detenido a delincuentes extraditen al delincuente o lo hagan comparecer ante la justicia; y exige que las partes se presten asistencia mutua en los procedimientos penales invocados con arreglo al Convenio[281].

3. Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil (1971): Establece que comete un delito quien ilícita e intencionalmente perpetre un acto de violencia contra una persona a bordo de una aeronave en vuelo si ese acto pudiera poner en peligro la seguridad de la aeronave; coloque un artefacto explosivo en una aeronave; o intente cometer esos actos; o sea cómplice de una persona que perpetre o intente perpetrar tales actos. Exige que las partes en el Convenio castiguen estos delitos con «penas severas» y exige que las partes que hayan detenido a los delincuentes extraditen al delincuente o lo hagan comparecer ante la justicia[282].

4. Protocolo para la represión de actos ilícitos de violencia en los aeropuertos que presten servicios a la aviación civil internacional, complementario del

[280] NACIONES UNIDAS. (1969). Convenio sobre los infractores y ciertos otros actos cometidos a bordo de las aeronaves, pp. 242-251. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv1-spanish.pdf

[281] NACIONES UNIDAS. (1973). Convenio para la represión del apoderamiento ilícito de aeronaves, pp. 123-127. Recuperado de : https://treaties.un.org/doc/db/Terrorism/Conv2-spanish.pdf

[282] NACIONES UNIDAS. (1975). Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, pp. 198-202. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv3-spanish.pdf

convenio para la represión de actos ilícitos contra la seguridad de la aviación civil (1988): Amplía las disposiciones del Convenio de Montreal para incluir los actos terroristas cometidos en los aeropuertos que prestan servicios a la aviación civil internacional[283].

5. Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional (2010): Tipifica como delito el acto de usar aeronaves civiles como armas para causar la muerte, lesiones o daños; tipifica como delito el acto de usar aeronaves civiles para descargar armas biológicas, químicas y nucleares o sustancias similares para causar la muerte, lesiones o daños, o el acto de usar estas sustancias para atacar una aeronave civil; tipifica como delito el transporte ilícito de armas biológicas, químicas y nucleares o determinados materiales conexos; un ataque cibernético dirigido contra instalaciones de navegación aérea constituye un delito; la amenaza de cometer un delito puede ser un delito en sí misma, si la amenaza es verosímil; el concierto para delinquir, o su equivalente, es punible[284].

6. Protocolo complementario del convenio para la represión del apoderamiento ilícito de aeronaves (2010): Complementa el convenio para la represión del apoderamiento ilícito de aeronavesampliando su alcance para abarcar diferentes formas de secuestro de aeronaves, incluso a través de medios tecnológicos modernos; incorpora las disposiciones del Convenio de *Beijing* relacionadas con una amenaza o conspiración para cometer un delito[285].

[283] NACIONES UNIDAS. (1990). Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, pp. 488-491. Recuperado de : https://treaties.un.org/doc/db/Terrorism/Conv7-spanish.pdf

[284] NACIONES UNIDAS. (2010a). Convenio de Beijing. Conjunto de textos administrativos para la ratificación del convenio para la represión de actos ilícitos contra la seguridad de la aviación internacional, pp. 1-5. Recuperado de: http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_ES.pdf

[285] NACIONES UNIDAS. (2010b). Protocolo de Beijing, Conjunto de textos administrativos para la ratificación del protocolo complementario del convenio para la represión del apoderamiento ilícito de aeronaves. Doc 9959 pp. 1-4. Recuperado de: http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_protocol_ES.pdf

7. Protocolo que modifica el convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves (2014)[286].

Instrumento sobre la protección de personal internacional

8. Convención sobre la prevención y el castigo de delitos contra personas internacionalmente protegidas, inclusive los agentes diplomáticos (1973): Entiende por "persona internacionalmente protegida" un Jefe de Estado, Ministro de Relaciones Exteriores, representante o funcionario de un Estado o una organización internacional que tenga derecho a protección especial en un Estado extranjero y sus familiares. Exige a las partes que tipifiquen como delito la comisión de un homicidio, secuestro u otro atentado contra la integridad física o la libertad de una persona internacionalmente protegida; la comisión de un atentado violento contra los locales oficiales, la residencia particular o los medios de transporte de tal persona; la amenaza o tentativa de cometer tal atentado; y de todo acto que constituya participación en calidad de cómplice y que los castiguen "con penas adecuadas en las que se tenga en cuenta" su carácter grave[287].

Instrumento sobre la toma de rehenes

9. Convención internacional contra la toma de rehenes (1979): Dispone que toda persona que se apodere de otra o la detenga, y amenace con matarla, herirla o mantenerla detenida a fin de obligar a un tercero, a saber, un Estado, una organización internacional intergubernamental, una persona natural o jurídica o un grupo de personas, a una acción u omisión como condición explícita o implícita para la liberación del rehén, comete el delito

[286] NACIONES UNIDAS. (2014). Protocolo de Montreal. Protocolo que modifica el convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, pp. 1-2. Recuperado de: http://www.icao.int/secretariat/legal/list%20of%20parties/montreal_prot_2014_es.pdf

[287] NACIONES UNIDAS. (1977). Convención sobre la prevención y el castigo de delitos contra personas internacionalmente protegidas, inclusive agentes diplomáticos, pp. 191-195, Recuperado de : https://treaties.un.org/doc/db/Terrorism/spanish-18-7.pdf

de toma de rehenes en el sentido de la presente Convención[288].

Instrumentos sobre el material nuclear

10. Convención sobre la protección física de los materiales nucleares (1980): Tipifica como delito la posesión, la utilización, la transferencia y el robo de materiales nucleares sin autorización legal, y la amenaza del empleo de materiales nucleares para causar la muerte o lesiones graves a una persona o daños materiales sustanciales[289].

11. Enmiendas a la convención sobre la protección física de los materiales nucleares (2005): Establecen la obligación jurídicamente vinculante de los Estados Partes de proteger las instalaciones y los materiales nucleares de uso nacional con fines pacíficos, así como su almacenamiento y transporte. Disponen una mayor cooperación entre los Estados con respecto a la aplicación de medidas rápidas para localizar y recuperar el material nuclear robado o de contrabando, mitigar cualquier consecuencia radiológica del sabotaje y prevenir y combatir los delitos conexos.

Instrumentos sobre la navegación marítima

12. Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima (1988): Establece un régimen jurídico aplicable a los actos cometidos contra la navegación marítima internacional parecido a los regímenes establecidos respecto de la aviación internacional. Dispone que comete delito la persona que ilícita e intencionalmente se apodere de un buque o ejerza el control sobre éste mediante violencia, amenaza o intimidación; cometa un acto de violencia contra una persona que se encuentre a bordo de un buque, si dicho acto puede poner en peligro la navegación segura del buque; coloque artefactos o sustancias destructivos a bordo de un buque; y perpetre otros actos contra la seguridad de los

[288] NACIONES UNIDAS. (1983). Convención internacional contra la toma de rehenes, pp. 238-243. Recuperado de : https://treaties.un.org/doc/db/Terrorism/spanish-18-5.pdf

[289] NACIONES UNIDAS. (1987). Convención sobre la protección física de los materiales nucleares, pp. 152-160., Recuperado de : https://treaties.un.org/doc/db/Terrorism/Conv6-spanish.pdf

buques[290].

13. Protocolo de 2005 del convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima (2005): Tipifica como delito la utilización de un buque como instrumento para favorecer la comisión de un acto de terrorismo. Tipifica como delito el transporte a bordo de un buque de diversos materiales a sabiendas de que se pretende usarlos para causar, o para amenazar con causar, la muerte, lesiones graves o daños, a fin de favorecer la comisión de un acto de terrorismo. Tipifica como delito el transporte a bordo de un buque de personas que han cometido actos de terrorismo, e introduce procedimientos para regular el embarque en un buque sospechoso de haber cometido un delito previsto por el Convenio.

14. Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental (1988): Establece un régimen jurídico aplicable a los actos realizados contra plataformas fijas emplazadas en la plataforma continental similar a los regímenes establecidos respecto de la aviación internacional[291].

15. Protocolo de 2005 relativo al protocolo de 1988 para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental (2005): Adapta los cambios en el Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima al contexto de las plataformas fijas emplazadas en la plataforma continental.

Instrumento sobre los materiales explosivos

16. Convenio sobre la marcación de explosivos plásticos para los fines de detección (1991): Su objetivo es controlar y limitar el empleo de explosivos plásticos no marcados e indetectables. Las partes están obligadas a

[290] NACIONES UNIDAS. (1992a). Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima, pp. 262-274. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv8-spanish.pdf

[291] NACIONES UNIDAS. (1992b). Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fíjas emplazadas en la plataforma continental, pp. 323-329. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv9-spanish.pdf

asegurar en sus respectivos territorios un control efectivo de los explosivos plásticos «sin marcar», es decir, los que no contengan uno de los agentes de detección enumerados en el anexo técnico del tratado. Cada una de las partes deberá, entre otras cosas: adoptar las medidas necesarias y eficaces para prohibir e impedir la fabricación de explosivos plásticos sin marcar; impedir la entrada o salida respecto de su territorio de explosivos plásticos sin marcar; ejercer un control estricto y efectivo sobre la tenencia y transferencia de explosivos sin marcar que se hayan fabricado o introducido en su territorio antes de la entrada en vigor del Convenio; asegurarse de que todas las existencias de esos explosivos sin marcar que no estén en poder de las autoridades militares o policiales se destruyan o consuman, se marquen o se transformen permanentemente en sustancias inertes dentro de un plazo de 3 años; adoptar las medidas necesarias para asegurar que los explosivos plásticos sin marcar que estén en poder de las autoridades militares o policiales se destruyan o consuman, se marquen o se transformen permanentemente en sustancias inertes dentro de un plazo de 15 años; y asegurar la destrucción, lo antes posible, de todo explosivo sin marcar fabricado después de la entrada en vigor del Convenio para ese Estado[292].

Instrumento sobre los atentados terroristas con explosivos

17. Convenio internacional para la represión de los atentados terroristas cometidos con bombas (1997): Crea un régimen de jurisdicción universal respecto de la utilización ilícita e intencional de explosivos y otros artefactos mortíferos en o contra diversos lugares concretos de uso público con la intención de matar u ocasionar graves lesiones físicas o con la intención de causar una destrucción significativa de ese lugar[293].

[292] NACIONES UNIDAS. (2010c). Convenio sobre la marcación de explosivos plásticos para los fines de detección, pp. 1-8. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv10-spanish.pdf

[293] NACIONES UNIDAS. (1998). Convenio internacional para la represión de los atentados terroristas cometidos con bombas, pp. 1-14. Recuperado de: https://treaties.un.org/doc/db/Terrorism/spanish-18-9.pdf

Instrumento sobre la financiación del terrorismo

18. Convenio internacional para la represión de la financiación del terrorismo (1999): Insta a las partes a que adopten medidas para prevenir y contrarrestar la financiación de terroristas, ya sea directa o indirectamente, por medio de grupos que proclamen intenciones caritativas, sociales o culturales o que se dediquen también a actividades ilícitas, como el tráfico de drogas o el contrabando de armas. Compromete a los Estados a exigir responsabilidad penal, civil o administrativa por esos actos a quienes financien el terrorismo; y prevé la identificación, congelación y confiscación de los fondos asignados para actividades terroristas, así como la distribución de los fondos decomisados entre los Estados afectados, en función de cada caso. El secreto bancario dejará de ser una justificación para negarse a cooperar[294].

Instrumento sobre el terrorismo nuclear

19. Convenio internacional para la represión de los actos de terrorismo nuclear (2005): Abarca una amplia gama de actos y posibles objetivos, entre ellos las centrales y los reactores nucleares; contempla la amenaza y la tentativa de cometer dichos delitos o de participar en ellos, en calidad de cómplice;establece que los delincuentes deberán ser enjuiciados o extraditados; alienta a los Estados a que cooperen en la prevención de atentados terroristas intercambiando información y prestándose asistencia mutua en las investigaciones penales y los procedimientos de extradición; y contempla tanto las situaciones de crisis (prestación de asistencia a los Estados para resolver la situación) como las situaciones posteriores a la crisis (disposición del material nuclear por conducto del Organismo Internacional de Energía Atómica (OIEA) a fin de garantizar su seguridad)[295].

[294] NACIONES UNIDAS. (1999). Convenio internacional para la represión de la financiación del terrorismo, pp. 1-19. Recuperado de : https://treaties.un.org/doc/db/Terrorism/spanish-18-11.pdf

[295] NACIONES UNIDAS. (2018) Actividades de lucha contra el terrorismo, instrumentos jurídicos internacionales. Recuperado de: http://www.un.org/es/counterterrorism/legal-instruments.shtml

IV.1.2.- Tratados en el ámbito de política exterior y seguridad común de la Unión Europea

Tratado de Maastricht (7 de febrero de1992). El TUE[296], viene a añadir otros dos pilares político-jurídicos de nuevo cuño, que él mismo regula: la política exterior y de seguridad común.

Tratado de Niza (14 de febrero de 2000). Fueron agregados los artículos 27 A a 27 E de cooperación reforzada en el ámbito de la política exterior y de seguridad común[297].

Tratado de Lisboa (18 de julio de 2010). Se amplían los artículos sobre la acción exterior, la política exterior y la seguridad común[298].

IV.1.3.- La OSCE (Organización para la Seguridad y la Cooperación en Europa)

La historia de la OSCE se remonta a los primeros años de la década de 1970, al Acta Final de Helsinki (1975) y a la creación de la Conferencia sobre la Seguridad y la Cooperación en Europa (CSCE), que durante la Guerra Fría se convirtió en un importante foro multilateral de diálogo y negociación entre el Este y Occidente.

[296] CONSEJO DE LAS COMUNIDADES EUROPEAS. (2010) Tratado de Maastrich sobre la Unidad Europea. Recuperado de: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_es.pdf

[297] EUROPEAN UNION. (22 de julio de 2015). EUR-Lex. Cooperaciones reforzadas. Recuperado de: https://es.wikipedia.org/wiki/EUR-Lex

[298] ALDECOA LUZARRAGA, F. y GUINEA LLORENTE, M. (20 de febrero de 2008). El rescate sustancial de la Constitución Europea a través del Tratado de Lisboa: la salida del laberinto. Documento de Trabajo nº 9, Real Instituto Elcano. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/europe/europa/home/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jjEBf3QG93QwMLLxMjA08jQxNDf0dTo1BjQ_2CbEdFAMD4gFE!/?WCM_PORTLET=PC_7_3TDGQKG108N000I2HUKBMI2OG3000000_WCM&WCM

La OSCE, con sus 57 Estados participantes en América del Norte, Europa y Asia, es la organización de seguridad regional más grande del mundo, que trabaja en pro de la estabilidad, la paz y la democracia de más de mil millones de personas a través del diálogo político sobre valores compartidos y de una labor práctica cuyos efectos son decisivos y duraderos.

Mediante la labor de sus Instituciones, unidades de expertos y su red de operaciones sobre el terreno, la OSCE aborda cuestiones que afectan directamente a nuestra seguridad común, entre ellas, el control de armamentos, la buena gobernanza, la seguridad energética, la trata de personas, la democratización, la libertad de los medios de comunicación y las minorías nacionales. En un plano más amplio, la OSCE aborda aquellos retos para la seguridad que suponen una amenaza transnacional, tales como el cambio climático, el terrorismo, la radicalización y el extremismo violento, la delincuencia organizada, el ciberdelito y el tráfico de drogas y armas, así como la trata de personas. Promueve la creación de unos vínculos y cooperación más sólidos entre los Estados y, para ello, establece asociaciones entre los sectores público y privado, además de fomentar la participación de la sociedad civil[299].

IV.1.4.- Manual de Tallin. Tratados en ciberseguridad de la OTAN

El CCD COE es un Centro de Excelencia que recoge la capacidad de Ciberdefensa de la OTAN, creado en el año 2008, en Tallín (Estonia), y que pretende aunar los esfuerzos de los países que patrocinan el centro: Estonia, Letonia, Lituania, Alemania, Hungría, Italia, Polonia, Eslovenia, España, Holanda y Estados Unidos.

El Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (CCD COE), publicó en 2017 el "Manual de Tallín" (*Tallinn Manual on the International Law Applicable to Cyber Warfare*), documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra. Es un Manual sobre ciberguerra y legislación internacional creado por el CCDCOE (OTAN) que tiene como objetivo crear un marco legal sobre la

[299] OSCE. (2016). Ver su Web: http://www.osce.org/es/whatistheosce/factsheet

ciberguerra basándose en el *International Institute of Humanitarian Laws*[300].

Cumbre de Riga, 29 de Noviembre de 2006

La Cumbre de Riga fue la primera Cumbre de la OTAN que destacó la necesidad de seguridad Cibernética. Los ataques cibernéticos se han convertido en una fuente de amenazas en el mundo globalizado en que vivimos. Así lo contemplan ya algunos países de nuestro entorno y diversas organizaciones internacionales, algunos de los cuales ya han elaborado estrategias de ciberseguridad o ciberdefensa. La OTAN ha sido consciente de este riesgo emergente y como tal lo ha tratado en la agenda de sus cumbres, empezando por la Cumbre de Riga de 2006[301].

Cumbre de Bucarest, 4 de Abril de 2018

- Nuevo paso de la OTAN en la ciberdefensa.
- Estonia sufrió un conjunto de ciberataques supuestamente respaldados por el Kremlin que colapsaron el país[302].
- En 2010 la OTAN estableció que los ciberataques constituían una de las nuevas amenazas a las que debía hacer frente.
- Las principales potencias cibernéticas son reticentes a compartir todo su arsenal cibernético con sus socios de la OTAN.
- Para no quedarse atrás, España necesita dar un significativo paso adelante en el desarrollo de cibercapacidades propias[303].

[300] OTAN. (2017).Tallinn Manual Process. NATO Cooperative Cyber Defense Centre of Excellense. Vid. https://ccdcoe.org/tallinn-manual.html

[301] CARO BEJARANO, M.J. (17 de marzo de 2011) Nuevo concepto de ciberdefensa de la OTAN. http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

[302] FERNÁNDEZ, R. (30 de mayo de 2009). Estonia, primera víctima de los hackers. *El País*. Recuperado de http://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

[303] COLOM, G. y FOJOM, E. (6 de julio de 2016). Nuevo paso de la OTAN en ciberdefensa. *Periódico digital El Español*. Recuperado de: http://www.elespanol.com/opinion/20160705/137856215_12.html

Cumbre de Lisboa, 20 de Noviembre de 2010

Se da un gran salto en ciberdefensa. Se redacta una estrategia y unos planes comunes en la defensa cibernética de los países que la componen y sus aliados.

El 10 de marzo de 2010, los Ministros de Defensa de la OTAN aprobaron el Nuevo Concepto de Ciberdefensa de la Alianza. Este concepto define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados.

También se destacó la importancia de cooperar con sus socios y otros organismos internacionales en ciberdefensa, y la necesidad de integrar las ciberamenazas en el planeamiento de defensa de la OTAN. Se acordó que los ministros de Defensa aprobarían una revisión de la Política de Ciberdefensa y una Acción de Ciberdefensa en la siguiente reunión en junio de 2010.

Durante la reunión, los Ministros de Defensa comprobaron el progreso de un conjunto de medidas que se decidieron en la Cumbre de Lisboa de noviembre de 2010 para conseguir que la Alianza sea más efectiva y eficiente a la hora de abordar las nuevas amenazas a la seguridad.

La OTAN realiza en este ámbito actividades de: coordinación y asesoramiento en ciberdefensa; asistencia a las Naciones; investigación y formación; y cooperación con los socios:

1) **Coordinación y asesoramiento en ciberdefensa**: La política de ciberdefensa se implementa mediante las autoridades políticas, militares y técnicas de la OTAN, así como por las naciones. La Autoridad para la Gestión de Ciberdefensa CDMA es la responsable de la coordinación de este ámbito dentro de la Alianza, centrándose particularmente en la amenaza cibernética; la gestión del riesgo de seguridad; la valoración de las vulnerabilidades; y la continuidad de negocio de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza. La creación de esta autoridad supuso un hito importante en el proceso de construcción de la ciberseguridad en la OTAN. Ante una emergencia cibernética ésta es la autoridad a la que se debe acudir dentro de la OTAN. Esta autoridad coordina a través del Consejo de Gestión de Ciberdefensa – CDMB, del que forman parte los líderes de los

comités político, militar, operacional y técnico de la OTAN con responsabilidades en ciberdefensa. Este consejo constituye el principal órgano de consulta de la OTAN en ciberdefensa y aconseja a los estados miembros. La autoridad opera bajo la División de Desafíos Emergentes de Seguridad. La misión de esta autoridad es revisar y coordinar las capacidades.

2) **Asistencia a las naciones**: Antes de los ciberataques de Estonia de 2007, los esfuerzos en ciberdefensa de la OTAN se concentraban principalmente en la protección de los sistemas de comunicación propios y los que eran operados por la Alianza. Tras estos ataques, que se dirigieron contra servicios públicos y se realizaron a través de Internet, el objetivo de la OTAN se ha ampliado hacia la ciberseguridad de las naciones aliadas. Para ello la OTAN ha desarrollado mecanismos para asistir a los aliados que soliciten su apoyo en la protección de sus sistemas de comunicación, a través de Equipos de Respuesta Rápida. No obstante, las naciones aliadas tienen la responsabilidad de la seguridad de sus sistemas de comunicación.

3) **Investigación y Formación:** El Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre of Excellence -CCDCOE) en Tallinn, Estonia fue acreditado en 2008. Este centro se encarga de la investigación y formación en ciberguerra con personal experto de los diez países que lo patrocinan (Estonia como país anfitrión, Alemania, Eslovaquia, España, EE.UU., Hungría, Italia, Letonia, Lituania y Turquía). Su misión es mejorar la capacidad y cooperación de la OTAN y sus estados miembros en Ciberdefensa mediante el desarrollo de programas y proyectos de I+D+i, formación, análisis de casos reales y consulta.

4) **Cooperación con los socios:** La OTAN también desarrolla una cooperación práctica en ciberdefensa según las guías del Consejo para Cooperación en Ciberdefensa con los socios y organizaciones internacionales (aprobado en agosto de 2008) y del Marco de Cooperación en Ciberdefensa entre OTAN y los países socios (aprobado en abril de 2009).

   La autoridad de gestión de ciberdefensa-CDMA apoyada, cuando es necesario, por el Comité de Planificación de Comunicación Civil, los Centros de Excelencia de Ciberdefensa de Tallinn y de Defensa contra el Terrorismo

de Ankara, así como el Programa de Ciencia por la Paz y la Seguridad, ha organizado charlas de expertos, investigaciones, seminarios de formación e intercambios de información entre los socios y organizaciones internacionales interesadas (la Unión Europea y la OSCE).

5) **Principales comités de decisión y de consejo**, la OTAN articula sus decisiones a través de los siguientes organismos internos:

- El Consejo del Atlántico Norte – el comité político de decisión a más alto nivel – .Tiene el control total sobre las políticas y actividades relativas a ciberdefensa.

- El Comité de Planeamiento y Política de Defensa – DPPC (*Defence Policy and Planning Committee*), que sustituyó al Grupo de Trabajo Ejecutivo en junio de 2010, ha desarrollado las propuestas a nivel político (es decir, preparación de una política de ciberdefensa y decisión OTAN sobre la creación de la Autoridad de Gestión de Ciberdefensa) para la aprobación por el Consejo.

- El Comité de Consulta, Mando y Control - NC3 (*NATO Consultation, Command and Control*) constituye el organismo principal de consulta de los aspectos técnicos y de implementación sobre ciberdefensa.

- Las Autoridades Militares – NMA (*NATO Military Authority*); la Agencia de Consulta, Mando y Control - NC3A (NATO C3 Agency) tienen la responsabilidad de identificar los requisitos operacionales y la adquisición e implementación de las capacidades de ciberdefensa y la Agencia de servicios de Información y Comunicación NCSA (*NATO Communication and Information Systems Services Agency*) a través de su centro técnico.[304].

[304] CARO BEJARANO, M.J. (17 de marzo de 2011). Gobierno de España, Ministerio de Defensa, IEES. Nuevo concepto de ciberdefensa de la OTAN, documento informativo del IEEE-09/2011: Recuperado de: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

Cumbre de Gales, 15 de Septiembre de 2014

La cumbre de la OTAN de Newport de 2014 (también llamada cumbre de Gales de 2014) fue celebrada los días 4 y 5 de septiembre de 2014 en Newport (Gales, Reino Unido). Los dos temas principales que trataron los 28 jefes de Estado y de gobierno fueron la crisis de Ucrania y la ofensiva en el norte de Irak del Estado Islámico (EE.UU. forja una alianza de 10 países para combatir a los yihadistas)[305].

Cumbre de Varsovia, 9 de julio de 2016

El 8 y 9 de julio de 2016, Varsovia, la capital polaca, albergó la cumbre de la Alianza Atlántica. Los altos cargos de la OTAN se reunieron para abordar la agenda internacional, la lucha antiterrorista y el futuro del bloque tras los cambios geopolíticos en Europa en un ámbito hostil debido a la retórica de "contención" de Occidente y al despliegue de más fuerzas militares cerca de las fronteras rusas.

Se celebró en Varsovia la Cumbre de Jefes de Estado o de Gobierno de la Alianza Atlántica. La agenda del encuentro cubrió numerosos aspectos de actualidad, la mayoría de ellos relacionados con la Federación Rusa (la creciente asertividad en su área de influencia y el empleo de estrategias híbridas, las relaciones entre la OTAN y Ucrania o el refuerzo de la presencia militar en los países bálticos), el compromiso suscrito en la Cumbre de Gales (2014) de incrementar el gasto en defensa de los veintiocho o la consolidación de la ciberdefensa aliada tres lustros después de que la OTAN tomara conciencia del valor estratégico del ciberespacio. La toma de conciencia de la Alianza Atlántica del potencial que posee el ciberespacio para el desarrollo de las operaciones militares se produjo en 1999. Coincidiendo con la Operación Fuerza Aliada en Kosovo y el bombardeo por error de la embajada china en Belgrado, *hacktivistas* serbios, rusos y chinos realizaron varios ataques de Denegación de Servicio y *defacements* sobre sus sitios web. Aunque irrelevantes, estos incidentes mediaron

[305] ABELLÁN, L. (5 de septiembre de 2014) EE UU forja una alianza de 10 países para combatir a los yihadistas. *El Pais*. Recuperado de :http://internacional.elpais.com/internacional/2014/09/05/actualidad/1409917501_927947.html

para que Bruselas considerara conveniente mejorar la protección de sus redes informáticas, aumentar las capacidades de sus miembros y cooperar con otros actores, especialmente la Unión Europea y el sector industrial.

Sin embargo, fue necesario esperar hasta la Cumbre de Praga (2002) para que la OTAN reconociera el valor intrínseco del ciberespacio. Condicionada por los trágicos sucesos del 11 de septiembre de 2001 y por el arranque del proceso de transformación militar, en la capital checa se tomaron varias iniciativas relevantes para la construcción de una ciberdefensa aliada. No sólo se reconoció la necesidad de incrementar la seguridad de los Sistemas de Información y Comunicaciones de la organización y se lanzó la *NATO Computer Incident Response Capability* (NCIRC) para prevenir, detectar y responder a ciberincidentes; sino que el Compromiso de Capacidades de Praga incluyó un paquete de medidas encaminadas a mejorar las cibercapacidades defensivas de la OTAN. Mientras NCIRC logró la plena capacidad operativa en 2014, el Paquete de Capacidades fue implementado de manera parcial, puesto que muchos países (desconocedores del valor intrínseco del ciberespacio para la seguridad nacional) solamente desarrollaron defensas pasivas.

Aunque la Guía de Política General – aprobada por el Consejo del Atlántico Norte en 2005 y refrendada en la Cumbre de Riga de 2006 para llenar el vacío estratégico existente entre los Conceptos Estratégicos de Washington (1999) y Lisboa (2010) – reconocía el valor intrínseco del ciberespacio para la seguridad euroatlántica, no fue hasta los ciberataques contra Estonia de 2007 cuando la OTAN tomó conciencia de los efectos técnicos y de las implicaciones políticas que podían tener este tipo de incidentes. Estonia quedó paralizada tras una campaña de ataques de Denegación de Servicio Distribuido (DDoS) realizados por hackers rusos, supuestamente coordinados desde el Kremlin. Como resultado, a principios de 2008 la OTAN aprobó el primer Concepto de Ciberdefensa y la Política de Ciberdefensa. Avalados en la Cumbre de Bucarest de Abril de 2008, donde se enfatizó "…la necesidad para la OTAN y las naciones de proteger los sistemas de información claves, compartir las mejores prácticas y proporcionar capacidades para asistir a los países aliados (bajo petición) para contrarrestar un ciberataque". Además, se desarrollaron los fundamentos de la ciberdefensa aliada con la llamada Ciberdefensa 1.0 y se establecieron tres pilares básicos en esta materia:

subsidiariedad (en caso de que no exista una petición previa para asistir al Estado víctima, se aplica el principio de responsabilidad exclusive de cada país soberano), no duplicación (para evitar que los esfuerzos se dupliquen) y seguridad (con el fin de garantizar la confianza mutua). Estas medidas motivaron que la ciberdefensa tuviese su propio espacio en la agenda de la OTAN a partir de la Cumbre de Lisboa de 2010.

En verano de 2008, durante el conflicto ruso-georgiano, se evidenció que los ciberataques podían apoyar las operaciones convencionales. Ello medió para que el Concepto Estratégico de la OTAN y la Declaración de la Cumbre de Lisboa de 2010 siguieran consolidando la ciberdefensa aliada. Los líderes de la OTAN reconocieron, entonces, que la dimensión cibernética estaría presente en los futuros conflictos, lo que fue determinante a la hora de aumentar las capacidades para detectar, evaluar, prevenir, defender y recuperarse de ciberataques. Para ello, se desarrolló el Paquete de Capacidades de Lisboa para suplir las brechas más importantes, incluyendo mejoras en el NCIRC. Con el objetivo de asistir a los aliados en materia de protección y respuesta, la OTAN estableció dos Equipos de Reacción Rápida que serían capaces de hacer frente a las crisis que atravesase la OTAN, así como de apoyar a las redes nacionales en caso de ser atacadas. Si bien proporcionan una limitada asistencia técnica (ayudando a proteger o restablecer los sistemas y coordinar la respuesta), tienen un fuerte valor político al afianzar el compromiso de la Alianza a la hora de apoyar sus propios sistemas y a los aliados. De esta forma, la OTAN sentaba las bases para integrar plenamente el elemento cibernético en las misiones de defensa colectiva, gestión de crisis y seguridad cooperativa.

Durante esta Cumbre, se le asignó al Consejo del Atlántico Norte la tarea de crear e implementar una política sobre ciberdefensa. De este modo, Lisboa supuso la formalización de la llamada Ciberdefensa 2.0, que derivó en la actualización de estructuras (tales como NCIRC), además de propiciar una respuesta de forma conjunta a los nuevos retos que plantea el ámbito virtual. La Cumbre de Lisboa elevó los ciberataques a la categoría que ostentan otro tipo de agresiones: la Política sobre Ciberdefensa contemplaba las ciberamenazas como posible causa de la activación del Artículo 5.

Más adelante, en 2011, se aprobó la política de la OTAN en materia de ciberdefensa. Un año después, se produjo la integración de la ciberdefensa en el Proceso de Planeamiento de Defensa de la OTAN. Asimismo, la ciberseguridad pasó a ser parte de la *Smart Defence* (iniciativa que supone que los aliados cooperen entre sí para generar, de forma efectiva y económicamente rentable, las modernas capacidades de defensa que la Alianza requiere) en la Cumbre de Chicago (2012). Ese mismo año, como fruto de la fusión de varias agencias de la Alianza, se creó la *NATO Communications and Information Agency* (NCIA) con el fin de apoyar el control, vigilancia e inteligencia de la Organización. Por otro lado, la OTAN llevó a cabo una serie de actualizaciones en el NCIRC. En 2013, la OTAN avocó por mejorar las capacidades cibernéticas a nivel nacional, que deben ser compatibles con las de la OTAN y los demás aliados, además de recordar a los Estados miembros que las capacidades de ciberdefensa de la Alianza cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y sus organismos asociados, estando a disposición de los aliados solo en caso de necesidad.

En 2014, los Ministros de Defensa de la OTAN aprobaron la nueva política sobre ciberdefensa, que está aún siendo implementada. Meses más tarde, durante la Cumbre de Gales (2014), los aliados acordaron que la ciberdefensa es uno de los principales elementos de la defensa colectiva, además de valorar su importancia para hacer frente a crisis y de cooperar en materia de seguridad. Si bien la OTAN debe centrarse en defender sus propias redes virtuales, los aliados se comprometieron a desarrollar las capacidades necesarias para proteger el ciberespacio a nivel nacional. Asimismo, teniendo en cuenta el compromiso de la OTAN con el cumplimiento del derecho internacional en todos los ámbitos, se determinó que es, por ende, aplicable al ciberespacio. Otro aspecto a destacar de esta Cumbre fue la decisión relativa al Artículo 5 del Tratado acerca de los ataques virtuales y una supuesta respuesta colectiva, que derivaría en una nueva Política de Ciberdefensa conocida como Ciberdefensa 3.0. Al respecto, se acordó que la activación del Artículo 5 en caso de un ataque cibernético contra uno de los miembros de la Organización se decidiría tras examinar cada caso en concreto. Por otro lado, la OTAN acuerda mejorar la cooperación con la industria, la compartición de información y la asistencia mutua entre los aliados, así como el

adiestramiento y ejercicios.

Tras la Cumbre, la OTAN reforzó su compromiso con la industria en el ámbito de la ciberseguridad, celebrándose un encuentro entre expertos en esta materia y representantes del sector privado para discutir acerca de las distintas formas de colaboración en la esfera del ciberespacio, durante el que se presentó el *NATO Industry Cyber Partnership* (NICP).

El refuerzo en la cooperación entre la OTAN y la Unión Europea (UE) en materia de ciberseguridad se materializó en febrero de 2016 con el "*Technical Arrangement on Cyber Defence*", que permite el intercambio de información entre los equipos de respuesta rápida. Recientemente, a mediados de junio de 2016, los ministros de defensa de los países miembros acordaron que el ciberespacio sería considerado una dimensión más junto con el aire, el mar y la tierra en la Cumbre de Varsovia. De esta forma, al dotar al ciberespacio de este rango, la OTAN podrá proteger de manera más eficaz sus misiones y operaciones. No obstante, la OTAN mantiene su postura defensiva y restrictiva, comprometiéndose a actuar de conformidad con el derecho internacional. Aunque en Varsovia se dará un nuevo impulso a la ciberdefensa aliada, todavía quedan algunas preguntas pendientes en esta materia: Homogeneizar las capacidades cibernéticas de los estados miembros: las capacidades de ciberdefensa aliadas cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y los organismos asociados de la Alianza, estando a disposición de los miembros en caso de necesidad, lo que hace necesario que los mismos aliados desarrollen sus propias capacidades de ciberdefensa. Sin embargo, el nivel de madurez de los miembros en esta materia es heterogénea y proporcional a su capacidad de asimilar la importancia estratégica de esta dimensión. Es por ello que muchos países están afrontando su adaptación al ciberespacio desde la urgencia de quien ha llegado tarde a este dominio y ello requiere mecanismos ágiles y robustos para llevar a cabo una gestión eficiente y eficaz del cambio. Precisamente, esta misma heterogeneidad en materia de cibercapacidades está provocando que algunas de las principales potencias cibernéticas de la OTAN (Estados Unidos, Reino Unido o Canadá, todas ellas pertenecientes al convenio *FiveEyes*) se muestren reticentes a desvelar todo su arsenal cibernético.

La Alianza sigue trabajando en la conceptualización de ciberataque y determinar el umbral a partir del cual éste debería ser calificado como una agresión contra un estado miembro y, por tanto, un supuesto contemplado por el Artículo 5. En la pasada cumbre ministerial, el Secretario General JENS STOLTENBERG declaró que un ciberataque severo podría ser constitutivo de una respuesta colectiva, aunque ello no ayuda mucho en resolver este asunto.

Del mismo modo, determinar la atribución de un ciberataque continúa siendo el principal problema con el que se encuentra la OTAN en este ámbito, puesto que hoy en día no es posible (desde un punto de vista tecnológico) determinar con certeza la procedencia de un ciberataque y la responsabilidad última del mismo. En este sentido, a pesar de que la Alianza está definiendo las opciones de respuesta ante un ciberataque enemigo (cibernética, convencional o la combinación de ambas) cabe preguntarse si un ciberataque presumiblemente llevado a cabo por una potencia adversaria implicaría una respuesta real, y mucho menos colectiva.

En definitiva, a pesar de que la ciberdefensa se ha consolidado definitivamente en la OTAN, son muchos los países miembros que todavía no disponen del mínimo de capacidades para protegerse (y mucho menos responder) en caso de ciberataques.

Es necesario que los aliados desarrollen capacidades específicas porque difícilmente podrán valerse de los medios propios de la OTAN o aprovecharse de las capacidades del resto de los miembros, muchos de ellos reticentes a exponer sus ciberfuerzas[306].

[306] REAL INSTITUTO ELCANO.(Julio de 2016). Informe mensual de Ciberseguridad. Estudios Internacionales y Estratégicos, THIBER, The Cyber Security Think Tank, *Ciber Elcano* Nº 16., Recuperado de: http://www.realinstitutoelcano.org/wps/wcm/connect/dc10afa8-a732-4b8d-a179-be83792d73a5/Ciber_Elcano_Num16.pdf?MOD=AJPERES&CACHEID=dc10afa8-a732-4b8d-a179-be83792d73a5

IV.1.5.- La OTAN y la UE aumentan la cooperación en ciberseguridad

Garantizar la seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de la mayoría de los Gobiernos, de la Unión Europea y de Organizaciones internacionales como la Organización del Tratado del Atlántico Norte (OTAN)[307].

Una de las partes esenciales de los sistemas de ciberseguridad Internacionales, Europeos y nacionales, que trabajan en la prevención, detección y respuesta a los riesgos que proceden del uso del ciberespacio, en el nivel puramente técnico, son los denominados Equipos de Respuesta a incidentes de Seguridad de la Información (CERTs). Mejorar la cooperación y el intercambio de información entre las CERT a nivel global es una de los principales desafíos a los que actualmente se enfrenta el campo de la ciberseguridad, tanto a nivel de Organizaciones públicas como privadas.

En este sentido, la OTAN, a través de su equipo de Capacidad de Respuesta de Incidentes Informáticos (NCIRC) y, el Equipo de Respuesta ante Incidentes de la Unión Europea (CERT-EU), firmaron el 10 de febrero de 2017 un Acuerdo Técnico de colaboración para fomentar el intercambio de información y buenas prácticas sobre procedimientos técnicos. La firma del Acuerdo se encuentra enmarcada como una de las prioridades establecidas en el marco Política de Defensa Cibernética de la Unión Europea en la línea de mejorar la cooperación con la OTAN en esta materia.

Otras acciones comunes en este ámbito, es la participación por parte de la UE en el ciber ejercicio anual que viene realizando la OTAN denominado "*Cyber Coalition*"[308].

[307] OTAN. (2018). North atlantic treaty organization. Organización del Tratado del Atlántico Norte. Vid. http://www.nato.int/

[308] OTAN. (18 de noviembre de 2015). Experts put to the test during NATO's largest annual cyber defence exercise.Organización del Tratado del Atlántico Norte.Recuperado de: http://www.nato.int/cps/en/natolive/news_124868.htm?selectedLocale=en

CAPÍTULO V

APLICACIÓN LEGISLATIVA. ESTUDIO DE CASOS

Para la realización de este capítulo, nos basaremos en 7 sentencias reales, algunas basadas en la Ley CP de 1995 y otras en su actualización de 2015.Nuestra intención es analizar todos los hechos acometidos en las sentencias así como la respuesta jurídica de éstas, y encuestar a mandos operativos de las fuerzas de seguridad que actúan en este tipo de casos, para obtener información de los puntos fuertes y débiles de la aplicación operativa de la Ley antes y después de su reforma. Igualmente encuestaremos a los encargados de aplicar esta ley, a los jueces y magistrados del Supremo encargados de analizar estos casos y redactar las sentencias que expondremos a continuación.

V.1.- SENTENCIA 119/2007

V.1.1.- Análisis de la Sentencia

ROJ: **STS 2251/2007** - ECLI:**ES:TS:2007:2251**
Nº Sentencia: **119/2007** Tipo Órgano: **Tribunal Supremo. Sala de lo Penal** Municipio: **Madrid** -- Sección: **1** Resumen: **Delito de integración en organización terrorista islámica. Presunción de inocencia, derecho al secreto de las comunicaciones, informes de inteligencia, principio acusatorio.**

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	Vicente Pons Gamón
FECHA:	07-01-2007
PROYECTO:	"Ciberterrorismo, legislación: aplicación y seguridad"
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	STS 2251/2007
	Nº de Recurso: 10461/2006 Nº de Resolución: 119/2007
FECHA y LOCALIDAD.	MADRID – 16-02-2007
PROCEDIMIENTO	Penal - procedimiento abreviado/sumario
MAGISTRADO PONENTE:	D. Andrés Martínez Arrieta.
DEMÁS MAGISTRADOS	D. Perfecto Andrés Ibáñez D. José Manuel Maza Martín D. Miguel Colmenero Menéndez de Luarca D. José Antonio Martín Pallín
VOTO PARTICULAR:	D. Perfecto Andrés Ibáñez D. José Antonio Martín Pallín

Ilustración 38: *STS 2251/2007.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. ANDRÉS MARTÍNEZ ARRIETA, demás magistrados D. JOSÉ MANUEL MAZA MARTIN y D. PERFECTO ANDRÉS IBÁÑEZ siendo este último el que integra el voto particular. El Juzgado Central de Instrucción nº 2, instruyó sumario 7/03 contra el acusado, por delito de pertenencia a banda armada, y una vez concluso lo remitió a la Audiencia Nacional, Sala de lo Penal, que con fecha 31 de marzo de dos mil seis dictó sentencia que condena al recurrente por un delito de pertenencia a grupo u organización terrorista, formalizando una impugnación que articula en ocho motivos. En síntesis (ilustración 38), el relato fáctico señala que el recurrente, siguiendo la estrategia marcada por la organización terrorista «Al Qaeda», decidió desarrollar un proyecto de divulgación de la ideología radical y fundamentalista del extremismo islámico y captar a personas musulmanas de todo el mundo, para lo cual estaba creando una página web donde difundir, a través de internet tales contenidos, incluyendo la divulgación de *fatwas* o decretos islámicos. Las *fatwas* son veredictos emitidos por los *sheihks* (o sabios musulmanes), de acuerdo con la *sharia*, que debe seguir un buen musulmán.

Así, cuando el acusado fue detenido el 13 de abril de 2002, se le intervinieron doce ordenadores, importante equipo informático que formaba una red informática completa, si bien todos los ordenadores no estaban conectados a la red, que denotaba un conocimiento informático avanzado, que excedía, en todo caso, el normal para un domicilio y cuya finalidad era la realización de aquella página web de divulgación de la ideología terrorista, proyecto que fue abortado por la actuación policial.

Al acusado a pesar del voto particular en su defensa y la estimación parcial del recurso por fallos cometidos con las órdenes judiciales de escuchas telefónicas (quedando anuladas parte de ellas), solo se le exime de las costas del recurso, manteniéndose las penas ya que el tribunal ratifica la condena del fallo de primera instancia. La base de la condena se mantiene y se condena al acusado como autor responsable de un delito de pertenencia a grupo u organización terrorista, ya definido y sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de diez años de prisión con la accesoria de inhabilitación especial para el derecho de empleo o cargo público por tiempo de diez años[309].

V.1.2.- Aspectos de interés

NORMA DEMANDADA
Delito de pertenencia a banda armada.
PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNAL SUPREMO

El hecho probado del que, reiteramos nuevamente, debe partirse en este cauce casacional, establece los siguientes elementos que son relevantes para la subsunción:

a) Que el recurrente seguía la estrategia de “Al Qaeda”.
b) Que decidió divulgar el contenido de la ideología radical y fundamentalista del extremismo islámico, incluidas las ya citadas

[309] Vid. STS Sala de lo Penal 2251/2007 de 16 de febrero de 2007.ECLI: ES: TS: 2007:2251. Madrid (España). Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=524250&links=&optimize=20070426&publicinterface=true

fatwas.

c) Que otra finalidad del recurrente con esta actividad era captar a personas musulmanas de todo el mundo.

d) Que en ejecución de este plan contactó con un alto miembro de "Al Qaeda" y con diversas personas de ideología radical extremista.

e) Que el proyecto final del acusado era crear una página web para difundir en internet el contenido del pensamiento de los *sheiks* más radicales que propugnaban la *yihad*, esto es la divulgación de la ideología terrorista que propugna "Al Qaeda".

f) Que esa ideología y concretamente las *fatwas* son la base de las acciones de la citada organización.

De estos elementos es posible extraer dos datos que determinan la naturaleza de su conducta como de pertenencia a organización terrorista y no de mera colaboración. Esos datos son, primero, que el recurrente seguía las directrices de la organización (sigue su estrategia y trata con un miembro de relevancia de ella) y segundo, que su actividad es la de proporcionar un fundamento ideológico (en este caso concreto, religioso) a la comisión de atentados terroristas. En este sentido, puede afirmarse que lapertenencia supone por sí misma una prestación de algún tipo de servicio para los fines de la banda, ya en el campo ideológico, económico, logístico, de aprovisionamiento o de ejecución de objetivos de mayor intensidad que las conductas de colaboración previstas.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

La representación del recurrente, formalizó el recurso, alegando los siguientes MOTIVOS:

- Derecho a un proceso con todas las garantías y proscribe la indefensión. Se renuncia. Al amparo del art. 5.4 LOPJ y art. 854 LECrim, por vulneración del principio acusatorio.

- Al amparo del art. 5.4 LOPJ y art. 854 LECrim por vulneración del derecho a la presunción de inocencia del art. 24.2 CE.

- Al amparo del art. 849.2 LECrim, por error en la apreciación de la prueba.

- Al amparo del art. 850.1º LECrim, por falta de práctica en el plenario de una serie de pruebas que fueron propuestas en tiempo y forma, inicialmente admitidas y que, ante su no práctica en el plenario, se formuló la pertinente protesta y concretamente, la testifical del Embajador del Reino de Arabia Saudita en España y de Dña. ARACELI, persona que medió para el alquiler de un piso en Madrid para el acusado.

- Al amparo del art. 849.1º LECrim por aplicación indebida de los arts. 515.2º y 516.2º del Cp. DE CASACIÓN

- Al amparo del art. 854 LECrim, en relación con el art. 5.4 LOPJ por vulneración del derecho al secreto de las comunicaciones reconocido en el art. 18 CE.

- Al amparo del art. 5.4 LOPJ en relación con el art. 24.2 y art. 18 CE.

- Al amparo del art. 5.4 LOPJ y art. 854 LECrim.

El artículo 576 CP, que define comportamientos propios de complicidad, y, por lo tanto, de naturaleza periférica en el marco de la actividad de las bandas terroristas, y que constituyen un auxilio o preparación de otro comportamiento (Sentencia nº 1346/2001, de 28 de junio).

DEMANDA

Primero.- El Juzgado Central de Instrucción nº 2, instruyó sumario 7/03 contra GERARDO, por delito de pertenencia a banda armada, y una vez concluso lo remitió a la Audiencia Nacional, Sala de lo Penal, que con fecha 31 de marzo de dos mil seis dictó sentencia que contiene los siguientes

HECHOS PROBADOS: Primero. La *fatwa* (o decreto islámico) es definida como el veredicto emitido de acuerdo con la *sharia* (o ley islámica) ante una situación nueva y que indica el comportamiento que debe seguir un buen musulmán. La organización terrorista Al Qaeda sustenta sus acciones en tal base ideológica: *fatwas* emitidas por *sheiks* o sabios musulmanes de su influencia que respaldan religiosamente sus acciones y que ofrecen implícitamente “un pasaporte al paraíso de los mártires” a cualquier musulmán que aniquile a los identificados

en tales decretos islámicos como enemigos del Islam. Todos los atentados realizados por terroristas islámicos se han sustentado en una *fatwa*. Sin *fatwa* no hay atentado. Ningún terrorista musulmán podrá utilizar la religión para justificar su acción violenta si no existe una *fatwa* que ampare tal acción. La existencia de tal decreto islámico es fundamental por cuanto determina que un acto terrorista libere o no al *shahid* (mártir) de cualquier freno moral y sentimiento de culpabilidad, de ahí su importancia y peligrosidad.

Segundo.- En 1998, el procesado GERARDO, mayor de edad y sin antecedentes penales, siguiendo la estrategia marcada por la organización terrorista Al Qaeda, decidió desarrollar un proyecto de divulgación de la ideología radical y fundamentalista del extremismo islámico, incluidas las citadas *fatwas* o decretos islámicos, para captar a personas musulmanas de todo el mundo. Así, cuando fue detenido el 13 de abril de 2002, estaba creando, para difundir en internet, una página web donde enseñar los contenidos del Islam más radical y extremista, aquel que propugna la *Yihad* en su acepción de guerra contra todos aquellos que no compartan sus creencias, sus prácticas religiosas y su forma de vida en cualquier parte del mundo. En ejecución de este plan y a tal fin, en el mes de abril de 1998 JOSÉ FRANCISCO (a) EVERARDO, alto miembro de Al Qaeda, contactó telefónicamente con el acusado GERARDO. Fruto de aquel contacto, los días 26 al 30 de mayo de 1998, se realizó una reunión en el domicilio del acusado Gerardo sito en la c/ PASEO, nº. 000 de la ciudad de Palma de Mallorca, a la que asistieron el citado JOSÉ FRANCISCO y DANIEL, también de ideología radical extremista, con la finalidad de realizar el mentado proyecto, que denominaron "Proyecto de Divulgación". Posteriormente, entre los días 9 al 13 de septiembre del mismo año hubo otra reunión en el mismo domicilio de Gerardo, a la que asistieron los citados JOSÉ FRANCISCO y DANIELjunto con el también extremista ALFONSO, que le entregó a GERARDO veintidós CD del *Sheik*JUAN FRANCISCO (debiendo destacarse los números 2, 5 y 22 en que se hace un llamamiento a la guerra contra los EE.UU. y los judíos). Con el mismo fin relatado, el acusado Gerardo -aparte de los citados JOSÉ FRANCISCO, DANIEL y ALFONSO- mantuvo relaciones con importantes miembros radicales extremistas. En concreto: *SHEIK ESTEBAN. *JOSÉ ANTONIO (a) GUILLERMO. *SHEIK DONATO. *LUIS ANDRÉS. *MATÍAS ("el tunecino"). Posteriormente, a principios de 2001, el acusado trasladó su

domicilio de Palma de Mallorca a Sant Joan Despí (Barcelona), por no estar de acuerdo con la vestimenta de las mujeres de aquella ciudad, por resultarle ofensiva y contraria a sus ideas religiosas. En la entrada y registro que se efectuó en su domicilio el día 13 de abril de 2002, se le intervinieron doce ordenadores, importante equipo informático que formaba una red informática completa, si bien todos los ordenadores no estaban conectados a la red, que denotaba un conocimiento informático avanzado, que excedía, en todo caso, el normal para un domicilio y cuya finalidad era la realización de aquella página web de divulgación de la ideología terrorista, proyecto que fue abortado por la actuación policial.

DECISIÓN

F A L L A M O S:

QUE DEBEMOS DECLARAR Y DECLARAMOS HABER LUGAR PARCIALMENTE AL RECURSO DE CASACIÓN por infracción de Ley y quebrantamiento de forma interpuesto por la representación del acusado GERARDO, contra la sentencia dictada el día 31 de marzo de dos mil seis por la Audiencia Nacional, Sala de lo Penal, en la causa seguida contra el mismo, por un delito de pertenencia a banda armada, que casamos y anulamos.(Se condenó a Gerardo como autor responsable de un delito de pertenencia a grupo u organización terrorista, ya definido y sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de diez años de prisión con la accesoria de inhabilitación especial para el derecho de empleo o cargo público por tiempo de diez años, así como al pago de costas). La estimación se refiere a los motivos por vulneración del secreto de las comunicaciones sin trascendencia en el fallo de la sentencia impugnada que confirmamos en su contenido condenatorio. Declarando de oficio el pago de las costas causadas en este recurso. Comuníquese esta resolución a la mencionada Audiencia a los efectos legales oportunos, con devolución de la causa. Así por esta nuestra sentencia, que se publicará en la Colección Legislativa lo pronunciamos, mandamos y firmamos ANDRÉS MARTÍNEZ ARRIETA, PERFECTO ANDRÉS IBÁÑEZ, JOSÉ MANUEL MAZA MARTÍN, MIGUEL COLMENERO MENÉNDEZ DE LUARCA, JOSÉ ANTONIO MARTÍN PALLÍN.

PUBLICACIÓN.- Leida y publicada ha sido la anterior sentencia por el Magistrado Ponente Excmo. Sr. D ANDRÉS MARTÍNEZ ARRIETA, estando celebrando audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Secretario certifico.

ARGUMENTO DE LA DECISIÓN
PROBLEMA JURÍDICO RESUELTO POR LA SENTENCIA

El problema jurídico: por todos y cada uno de los argumentos de la fiscalía podemos determinar si el acusado pertenece o no a banda armada. En la sentencia se prueban hechos como:

- El de reunión del acusado con dirigentes de banda armada.
- Encontrar documentación relacionada con banda armada.
- Encontrar aparatos u ordenadores para llevar a cabo su cometido de creación WEB con fines de reclutar y enaltecer el terrorismo.
- Se cometen fallos con las órdenes judiciales de escuchas telefónicas quedando anulada parte de ellas.
- Es decir, el tribunal resuelve una parte a favor del acusado pero en conjunto ratifica la condena por pertenencia a banda armada.
- En definitiva el recurso se estima parcialmente, lo cual no es suficiente para no condenar al acusado ya que el tribunal ratifica la condena del fallo de primera instancia.

RATIO DECIDENDI (rd) “la razón de la decisión”

La sentencia objeto de la presente censura casacional condena al recurrente por un delito de pertenencia a grupo u organización terrorista, formalizando una impugnación que articula en ocho motivos. En síntesis, el relato fáctico señala que el recurrente, siguiendo la estrategia marcada por la organización terrorista «Al Qaeda», decidió desarrollar un proyecto de divulgación de la ideología radical y fundamentalista del extremismo islámico y captar a personas musulmanas de todo el mundo, para lo cual, estaba creando una página web donde difundir, a través de internet, tales contenidos, incluyendo la divulgación de *fatwas* o decretos islámicos. Las *fatwas* son veredictos emitidos por los *sheihks* (o sabios musulmanes), de acuerdo con la *sharia*, ante una situación

nueva, indicando el comportamiento que debe seguir un buen musulmán.

Estos decretos sustentan los atentados realizados por terroristas islámicos, de modo que ningún terrorista puede utilizar la religión para justificar su acción violenta si no existe una *fatwa* que la ampare. Ello en la medida en que su existencia determina que un acto terrorista libere o no al *shahid* (mártir) de cualquier freno moral o sentimiento de culpabilidad. El relato indica que la organización terrorista "Al Qaeda" sustenta sus acciones en esta base ideológica.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

El Tribunal une toda la información desde sus comienzos: el acusado se reúne repetidas veces con altos dirigentes de bandas armadas, cambia de domicilio y prepara un piso conjuntamente con aparatos informáticos, y nunca deja de tener contacto con la organización. Todo esto hace decidir al tribunal su culpabilidad.

VOTO PARTICULAR (SV)

La disidencia se centra en torno a la calificación jurídica de los hechos probados cuyo contenido asumimos en su integridad.

Descartadas las valoraciones teóricas sobre la doctrina islámica y su incidencia sobre actividades terroristas de organizaciones como Al Qaeda universalmente conocidas, nuestra disconformidad radica en la valoración jurídica de los hechos que se imputan o atribuyen al recurrente.

Con estos precedentes fácticos, la sentencia condena al recurrente como autor de un delito de integración en organización o grupo terrorista. Aplica los artículos 515.2º y 516 estimando la modalidad agravada de fin o propósito de subvertir el orden constitucional o alterar gravemente la paz social.

La propia sentencia cita jurisprudencia de esta Sala en la que se exige la existencia de un substrato primario, una pluralidad de personas, la existencia de unos vínculos entre ellas y el establecimiento de cierta jerarquía y organización.

La inexistencia de vínculos y la obediencia jerárquica se pone de relieve si se declara que desde 1998 hasta tres años y siete meses después el acusado no realizó actividad alguna a pesar de que recibió los CD que se entregan en 1998.

En nuestra opinión se ha quebrantado el principio de legalidad ya que se aplica la integración en organización terrorista sin que conste el soporte fáctico que permita llegar a esta conclusión.

En todo caso su misión, largamente demorada parece que con la complacencia y consentimiento de la organización ni siquiera se había llevado a efecto, ya que se encontraba en estado embrionario. Su misión, si es que así se había convenido, consistía en difundir ideas sobre el islamismo que pudieran ser controvertidas o sometidas a revisión crítica por algunos sectores mas racionales del Islam, pero en ningún caso se llegaron a plasmar en una efectiva difusión.

En definitiva nos encontramos ante una persona que, habiendo aceptado voluntariamente determinadas doctrinas xenófobas, de intransigencia y odio hacia otras religiones, trataba de difundirlas. Quizá podría tener encaje como conducta individual en alguna figura de difusión del odio o enaltecimiento del terrorismo, pero no de integración en banda armada.

V.2.- SENTENCIA 888/2007

V.2.1.- Análisis de la Sentencia

ROJ: STS 6998/2007 - ECLI:ES:TS:2007:6998
Nº Sentencia: 888/2007 Tipo Órgano: Tribunal Supremo. Sala de lo Penal. Municipio: Madrid -- Sección: 1 Resumen: Terrorismo. Derecho a un proceso con todas las garantías. Principio acusatorio. Presunción de inocencia. Prueba indiciaria. Falsificación con fines terroristas. Integración en banda terrorista. Motivación de la pena. Error en la apreciación de la prueba.

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	Vicente Pons Gamón
FECHA:	07-01-2007
PROYECTO:	“ciberterrorismo, legislación: aplicación y seguridad”

CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	STS 6998/2007
	Nº de Recurso: 10437/2007 Nº de Resolución: 888/2007
FECHA y LOCALIDAD.	MADRID – 25/10/2007
PROCEDIMIENTO	Penal - apelacion procedimiento abreviado
MAGISTRADO PONENTE:	D. Carlos Granados Pérez
DEMÁS MAGISTRADOS	D. Carlos Granados Pérez D. Perfecto Andrés Ibáñez D. José Ramón Soriano Soriano D. José Manuel Maza Martín
VOTO PARTICULAR:	NO SE REALIZA VOTO PARTICULAR

Ilustración 39: *STS 6998/2007.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. CARLOS GRANADOS PÉREZ, demás magistrados: D. PERFECTO ANDRÉS IBÁÑEZ, D. JOSÉ RAMÓN SORIANO SORIANO, D. JOSÉ MANUEL MAZA MARTÍN y MANUEL MARCHENA GÓMEZ, sin que se tenga constancia de voto particular. El Juzgado Central de Instrucción número 1 instruyó Sumario con el número 3/2004 y una vez concluso fue elevado a la Sala de lo Penal de la Audiencia Nacional, que con fecha 7 de febrero de 2007, dictó sentencia contra cinco acusados (dos de ellos detenidos y juzgados en Francia) por el delito de falsedad con finalidad terrorista y por el delito de pertenencia a organización terrorista condenándolos a 3 años de prisión y una multa de 12 meses por el primero y a 10 años de prisión e inhabilitación absoluta por el segundo (ilustración 39).

Todos los acusados son nacidos en la ciudad argelina de Chlef. Huyeron de Argelia, entre 1998 y 1999, al estar perseguidos como terroristas por las autoridades de dicho país, refugiándose en España, donde se reagruparon, constituyendo una célula u organización terrorista. Esta célula o grupo terrorista tenía como objetivos: la difusión del ideario extremista islámico, el proselitismo y captación de seguidores entre la población musulmana en España, la creación de domicilios que sirviesen de refugio a los miembros combatientes perseguidos en otros países al tiempo que de escondite y depósito de material electrónico,

informático, bacteriológico o químico, en su caso, preciso para la perpetración de atentados, el apoyo y ayuda a los compañeros presos, la compra y difusión de material de comunicaciones, facilitar a sus miembros, así como a otros miembros del radicalismo islámico de otros países que lo precisen, documentación falsa que facilitase su integración y ocultación entre la población musulmana y, finalmente, estar disponibles y preparados para pasar a la acción y atentar.

Los magistrados del Tribunal Supremo, estiman los recursos parcialmente y se dicta una nueva sentencia declarándose de oficio las costas.

"DEBEMOS DECLARAR Y DECLARAMOS HABER LUGAR PARCIALMENTE A LOS RECURSOS DE CASACIÓN por infracción de preceptos constitucionales e infracción de Ley interpuesto: Procede, en consecuencia, dejar sin efecto las condenas impuestas a los acusados JOSÉ ANTONIO y MIGUEL (detenidos y juzgados en Francia) por el delito de falsedad con finalidad terrorista, absolviéndoles de este delito y declarándose de oficio la parte correspondiente de las costas. Asimismo, acorde con los razonamientos expresados en la primera sentencia de casación, procede sustituir las penas impuestas a los acusados EVERARDO, ÁNGEL, JUAN CARLOS, por el delito de pertenencia a organización terrorista, que lo fue de diez años de prisión, con la accesoria de inhabilitación absoluta durante el tiempo de la condena, a cada uno de ellos, por la de SEIS AÑOS DE PRISIÓN e inhabilitación especial para empleo o cargo público por tiempo de seis años, a cada uno de los acusados. Respecto al delito de falsedad con finalidad terrorista, se sustituyen las penas impuestas a los acusados EVERARDO, ÁNGEL Y JUAN CARLOS, de tres años de prisión y multa de doce meses, por la de UN AÑO Y NUEVE MESES DE PRISIÓN Y MULTA DE SEIS MESES, a cada uno de estos tres acusados, con la misma cuota diaria fijada en la sentencia de instancia"[310].

[310] Vid. STS Sala de lo penal nº 888 de 25 de octubre de 2007. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=266351&links=&optimize=20071115&publicinterface=true

V.2.2.- Aspectos de interés

NORMA DEMANDADA
Pertenencia a organización terrorista y falsedad documental
PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNAL SUPREMO

Motivos de estimación de los diferentes recursos:

PRIMERO.- Formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

TERCERO.- Formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP. Se alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

CUARTO.- Formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se alega, en defensa del motivo, que ni en los hechos que se declaran probados ni en los fundamentos jurídicos de la sentencia recurrida se expresa que el ahora recurrente tuviera documentación falsificada.

QUINTO.- Formalizado al amparo del número 2º del artículo 849 LECrim, se invoca error en la apreciación de la prueba basado en documentos que obran en autos que demuestran la equivocación del juzgador sin resultar contradichos por otros elementos probatorios.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

RECURSO INTERPUESTO POR Everardo:

PRIMERO.- En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Se renuncia.

TERCERO.- Se renuncia.

CUARTO.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

QUINTO.- En el quinto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

SEXTO.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se niega la existencia de conducta que pueda ser subsumida en un delito de falsificación con finalidad terrorista.

SÉPTIMO.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Se alega, en defensa del motivo, que el relato de hechos probados no contiene conductas idóneas para poner en auténtico peligro la convivencia pacífica de la sociedad, subvertir el orden constitucional o alterar gravemente la paz pública ni referencia al requisito subjetivo ni la participación de los acusados en los fines de esa organización, por lo que no concurren los elementos que caracterizan al delito de integración en organización terrorista.

OCTAVO.- En el octavo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

Se alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

RECURSO INTERPUESTO POR ÁNGEL:

PRIMERO.- En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Se renuncia.

TERCERO.- Se renuncia.

CUARTO.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

QUINTO.- En el quinto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

SEXTO.- En el sexto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

SÉPTIMO.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se alega, respecto al delito de falsificación.

OCTAVO.- En el octavo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida,

de los artículos 515.2 y 516.2 CP.

Se alega, no concurren los elementos que caracterizan al delito de integración en organización terrorista.

NOVENO.- En el noveno motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP. Se alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

RECURSO INTERPUESTO POR JUAN CARLOS:

PRIMERO.- En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Se renuncia.

TERCERO.- Se renuncia.

CUARTO.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

QUINTO.- En el quinto motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se alega, respecto al delito de falsificación.

SEXTO.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP. Coincidiendo con los anteriores recursos, se alega que el relato de hechos probados no contiene conductas idóneas para poner en auténtico peligro la convivencia pacífica de la sociedad, subvertir el orden constitucional o alterar gravemente la paz pública ni referencia al requisito subjetivo ni la participación de los acusados en los fines de esa organización, por

lo que no concurren los elementos que caracterizan al delito de integración en organización terrorista.

SÉPTIMO.- En el séptimo motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP. Como los otros recurrentes, también alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

RECURSO INTERPUESTO POR JOSÉ ANTONIO

PRIMERO.- En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Se renuncia.

TERCERO.- Se renuncia.

CUARTO.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

QUINTO.- En el quinto motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se alega, en defensa del motivo, que ni en los hechos que se declaran probados ni en los fundamentos jurídicos de la sentencia recurrida se expresa que el ahora recurrente tuviera documentación falsificada.

SEXTO.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP. Como los otros recurrentes, alega que el relato de hechos probados no contiene conductas idóneas para poner en auténtico peligro la convivencia pacífica de la sociedad, subvertir el orden constitucional o alterar gravemente la paz pública ni referencia al requisito subjetivo ni la participación de

los acusados en los fines de esa organización, por lo que no concurren los elementos que caracterizan al delito de integración en organización terrorista.

SÉPTIMO.- En el séptimo motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

Como los otros recurrentes, también alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

RECURSO INTERPUESTO POR MIGUEL:

PRIMERO.- En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

SEGUNDO.- Se renuncia.

TERCERO.- Se renuncia.

CUARTO.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

QUINTO.- En el quinto motivo del recurso, formalizado al amparo del nº 2º del artículo 849 LECrim, se invoca error en la apreciación de la prueba basado en documentos que obran en autos que demuestran la equivocación del juzgador sin resultar contradichos por otros elementos probatorios.

SEXTO.- En el sexto motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP. Se niega la existencia de un delito de falsedad ya que no hay conducta falsaria con la realización de una fotocopia en color del permiso de residencia. El motivo debe ser estimado.

SÉPTIMO.- En el séptimo motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP. Como los otros recurrentes, alega que el relato de hechos probados no contiene conductas idóneas para poner en auténtico peligro la convivencia pacífica de la sociedad, subvertir el orden constitucional o alterar gravemente la paz pública ni referencia al requisito subjetivo ni la participación de los acusados en los fines de esa organización, por lo que no concurren los elementos que caracterizan al delito de integración en organización terrorista.

OCTAVO.- En el octavo motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP. Como los otros recurrentes, también alega que las penas se han impuesto con una insuficiente motivación, siendo inadecuados los elementos valorados y sin atender a la individualización de las circunstancias personales de cada uno de los acusados.

En los recursos realizados por los diferentes acusados la coincidencia de este motivo con idénticos formalizados por los anteriores recurrentes determina que deba dársele la misma respuesta y que proceda su estimación con el alcance que en ellos se deja expresado.

DEMANDA

1.- El Juzgado Central de Instrucción número 1 instruyó Sumario con el nº 3/2004 y una vez concluso fue elevado a la Sala de lo Penal de la Audiencia Nacional que, con fecha 7 de febrero de 2007, dictó sentencia que contiene los siguientes

HECHOS PROBADOS: "EVERARDO, (Conocido también como PAULÍN,JOAQUÍN), JUAN CARLOS (que en España está identificado con la identidad de IMANOL o ENRIQUE) y ÁNGEL, alias "Pitufo", también conocido con el nombre de DIEGO, todos ellos nacidos en la ciudad argelina de Chlef, pertenecientes todos ellos al grupo guerrillero "forkane", que desde una posición defensora del fundamentalismo islámico, lucharon en las montañas de la provincia argelina del Chelf en contra del GIA y del ejército argelino, integrados dentro de la organización" D.H.D.S. (*Djama Houumat Edaawa Essalafia*, esto es: Grupo de

Partidarios de la Corriente Salafista), huyeron de Argelia, entre 1998 y 1999, al estar perseguidos como terroristas por las autoridades de dicho país, refugiándose en España, donde se reagruparon, constituyendo una célula u organización terrorista en la que se integraron, JOSÉ ANTONIO y MIGUEL, el primero de ellos técnico de electrónica y el segundo diplomado en informática, opción ofimática. Junto a ellos formaban parte de esta célula española otros individuos, a los que no afecta la presente resolución, al haber sido detenidos en Francia, en estrecho contacto con otros individuos radicales islámicos, asentados en Francia, Alemania e Inglaterra. Esta célula o grupo terrorista tenía como objetivos: la difusión del ideario extremista islámico, el proselitismo y captación de seguidores entre la población musulmana en España, la creación de domicilios que sirviesen de refugio a los miembros combatientes perseguidos en otros países al tiempo que de escondite y depósito de material electrónico, informático, bacteriológico o químico, en su caso, preciso para la perpetración de atentados, el apoyo y ayuda a los compañeros presos, la compra y difusión de material de comunicaciones, facilitar a sus miembros, así como a otros miembros del radicalismo islámico de otros países que lo precisasen, documentación falsa que facilitase su integración y ocultación entre la población musulmana y, finalmente, estar disponibles y preparados para pasar a la acción. Así:

1.- El día 10 de agosto de 2002, EVERARDO adquirió, en unión de otros individuos no identificados, dos emisoras de radio de largo alcance, destinadas a los individuos detenidos en Francia por su integración en un grupo terrorista islámico.

2.- A disposición de Everardo, en el domicilio de MAURICIO (alias JUAN CARLOS), sito en la CALLE 000 nº.000, bajo, de Santa Coloma de Gramanet, se incautaron: 1 regulador de mezcla de oxígeno y acetileno, soldadores eléctricos, destornilladores de precisión, 1 texter de comprobación de carga, 1 reloj digital dual manipulado del que sale un cable al exterior, un conector Jack con los cables cortados, temporizadores eléctricos con relojes digitales, tipo PQS, material electrónico diverso manipulado, 1 portafusible de bayoneta con fusible, 1 fusible aéreo, 1 pulsador, una tarjeta musical. En el mismo domicilio, y, entre los efectos de su propiedad, se incautó un fax, remitido por JOSÉ MANUEL, en el que se le pide que le facilite un permiso de residencia y trabajo para regularizar su estancia en

territorio español.

3.- A disposición de EVERARDO, se incautó documentación consistente en un listado de datos de ciudadanos argelinos (nombres apellidos, situación documental en España), siete folios de datos, con el nombre de EVERARDO, en la parte superior de todos ellos, tramitados a través de la gestoría de Dña. EVA.

4.- En el piso alquilado por Everardo, DIRECCIÓN 000 nº. 001, se dio de alta en el censo de Barcelona JOSÉ MANUEL, de la célula de la *Courneuve* (Fr.), con la identidad falsa de SILVIO. Dicho individuo fue detenido en la Courneuve (Francia) imputándose su integración en una célula terrorista islámica.

5.- En el domicilio de EVERARDO, sito en Barcelona, CALLE 001 nº. 002. nº. 003, se refugiaron, durante su estancia en España, varias personas a las que se imputa su integración en una célula fundamentalista islámica francesa. Entre ellos, JESÚS LUIS, quien en septiembre de 2001 estuvo una semana en su casa, y en dicho domicilio se incautó documentación perteneciente a algunos de tales miembros, entre ella, permiso de residencia y trabajo, y siete documentos más, a nombre de ARTURO, y, un sobre, remitidos por ANDRÉS (imputado en Francia como perteneciente a la célula francesa de *Romainville*) dirigido a Pitufo, a la CALLE 002 nº. 004 de Bañolas, con tres fotografías de carnet en un grupo de cuatro de la que faltaba una.

6.- En el domicilio de JUAN CARLOS, sito en la CALLE 002 nº. 004 de Banyoles (es un domicilio con salida trasera, que da a la CALLE 003 nº. 005de la misma población) se encontró diversa documentación a nombre de personas imputadas en Francia como miembros de la célula francesa, en concreto, tarjeta de la seguridad social y diferentes documentos laborables de JUAN PABLO.

7.- En el domicilio de JUAN CARLOS, estaba preparada una caja, dirigida al detenido en Francia, JUAN PABLO, con destino a éste, a una prisión de Francia.

8.- En el domicilio de JUAN CARLOS, que compartía entonces con Pitufo, estuvo pernoctando FRANCISCO cuando éste estuvo en España en diciembre de 2002, y JUAN CARLOS, junto con Pitufo, lo llevaron a la estación de Gerona, a fin de que cogiese el tren con destino a Francia.

9.- En la habitación de JUAN CARLOS se incauta un CD, con 18 ficheros, con imágenes de la Yihad (Guerra Santa) y discursos de líderes radicales del fundamentalismo islámico, como JOSÉ ÁNGEL, que llaman a la participación en la Yihad. Documental denominado "la lucha"con escenas de campos de batalla mujahadines, de la guerra de Bosnia, Kósovo y Sarajevo.

10.- JOSÉ ANTONIO, con el mismo domicilio en Bañolas, recibe cartas de los detenidos en Francia.

11.- JOSÉ ANTONIO aparece, en una cinta de vídeo intervenida en el domicilio de EVERARDO, en compañía de JUAN PABLO (detenido en Francia).

12.- En el domicilio de la CALLE 002, nº. 004 de Bañolas, ocupado por JUAN CARLOS, JOSÉ ANTONIO, e MIGUEL se intervino diverso material como 1 amperímetro, soldadores, placas de circuitos, elementos electrónicos de radio portátil.

13.- MIGUEL y Pitufo, se desplazan a 22 de kilómetros de Bañolas, para desprenderse de documentación perteneciente a varios de los detenidos en Francia, acusados de pertenecer a una célula terrorista islámica francesa, entre ella, documentación de JUAN PABLO, MANUEL, RODOLFO y VÍCTOR.

14.- En el domicilio de Pitufo, sito en Olot CALLE 004 nº. 006- nº. 007, se incautó un teléfono móvil de la marca Trium nº. 008, con su pila, manipulado, al que se le habían practicado dos pequeños orificios en su parte superior, no utilizado como teléfono porque le falta la correspondiente tarjeta, hábil para ser utilizado como receptor de señal de un artefacto explosivo y tres walki-talkies motorola GP340, con sus cargadores y accesorios, adquiridos en Francia, manipulados en frecuencia y radio de alcance.

15.- A disposición de Pitufo y de su propiedad, se incautó, en el domicilio de BRUNO una mochila negra, en cuyo interior habían varias cintas de vídeo, cuyo contenido era una entrevista a GUSTAVO (también conocido como Jon) "La mañana sagrada" reportaje sobre la intifada palestina con imágenes de muertos y heridos palestinos, una conferencia de CHEIK ALQARMI "los valores de sacrificio" con imágenes del atentado del 11-S (EE.UU.) y una entrevista al militante suicida de RUBÉN, y dos cintas de charlas de JOSÉ ÁNGEL, líder religioso estrechamente

relacionado a la Yihad islámica, detenido en reino Unido desde el 13 de febrero de 2001 por terrorismo. El 16 de Diciembre de 2002, en La Courneuve, (Francia) fueron detenidos JOSÉ MANUEL, ALONSO, JUAN PABLO, y ILDEFONSO, por su pertenencia al grupo conocido como "célula de la Courneuve". El primero de ellos, tras haber estado durante su estancia en Georgia, en estrecha relación con los responsables de Al Qaeda. El día 17 de diciembre de 2002, JUAN CARLOS tira en un contenedor fotografías y *curriculums* de FRANCISCO y de CORNELIO, detenidos en Francia acusados de pertenecer al movimiento integrista islámico francés. Y, MIGUEL, en compañía de Pitufo, se desplazan 22 kilómetros, para deshacerse de documentación diversa de otros individuos, igualmente detenidos en Francia acusados de integrar un grupo terrorista de tendencia fundamentalista islámica, entre otros, de JUAN PABLO. El día 21 de Diciembre es detenido en la frontera franco-española Francisco, cuando éste, tras refugiarse en España para huir de la policía francesa, en la casa de Pitufo (ÁNGEL) y JUAN CARLOS (IMANOL), en Bañolas, CALLE 002 nº. 004, decide volver a Francia por encontrarse también inseguro en este refugio, tras haber estado en Georgia en estrecha relación con los responsables de Al Qaeda, así como en estrecha vinculación con los otros individuos detenido en Francia, habiendo ejercido actividades de apoyo a la Yihad chechena, dentro de un grupo muyahedin con base en el valle de Pankissi. JUAN CARLOS (IMANOL) tenía en su poder un pasaporte argelino, a nombre de Imanol, falso. Los sellos (tampones) falsos, utilizados en la falsificación del pasaporte de Imanol, se incautaron en el domicilio de Pitufo. En el domicilio de EVERARDO, se incautaron tampones de tinta, tinta para los tampones, sellos oficiales argelinos, sellos oficiales franceses, y sellos fechadores de distintos tamaños, una remachadora "ratio" con remaches de distintos tamaños, empleados en los pasaportes, así como fotografías de carnet de JOSÉ MANUEL FRANCISCO y JUAN PABLO, todos ellos detenidos en Francia como integrantes de las células francesas, y dos pasaportes y documentación falsa a nombre de CORNELIO y JOSÉ siendo EVERARDO, el encargado, dentro de la organización de la fabricación y obtención de documentación falsa para los distintos miembros de las células radicales europeas que lo precisaran. MIGUEL tenía en su poder, un permiso de residencia, falso, a su nombre, realizado mediante un sistema de reproducción fotomecánica de otro previamente digitalizado. ÁNGEL, *alias* Pitufo, *alias* DIEGO, tenía en su poder una licencia de conducir ciclomotores, y tarjetas de la Seguridad social, a nombre

de DIEGO, totalmente falsas, en la que aparece su fotografía, pese a que el verdadero Diego es otra persona que vive en la actualidad en Argelia, de donde no consta que haya salido. El día 24 de Diciembre de 2002, ALONSO, mayor de edad, con domicilio en la CALLE 005 nº.009, de Sant Jaume de Llierca (Gerona), ingeniero técnico de electricidad, accedió a llevar a DIEGO, *alias* Pitufo a Francia, eludiendo las carreteras principales, pues éste se lo pidió, para poder ver a su hijo en Navidad, sin que conste que ALONSO tuviese para ello más finalidad que la de ayudar a un conocido".

2.- La SENTENCIA DE INSTANCIA dictó el siguiente pronunciamiento:

FALLO: En atención a lo expuesto, y por la autoridad que nos confiere la CE, HEMOS DECIDIDO: Que debemos ABSOLVER y ABSOLVEMOS a ALONSO, de los delitos de pertenencia a organización terrorista, tenencia de explosivos y falsedad de documento público por los que venía siendo acusado en este procedimiento, con toda clase de pronunciamientos favorables, y declarando de oficio tres diecinueveavas partes de las costas procesales en él causadas.

Que debemos ABSOLVER y ABSOLVEMOS: a EVERARDO, a JUAN CARLOS (*alias* IMANOL), a JOSÉ ANTONIO, a MIGUEL, y a ÁNGEL (*alias* Pitufo, *alias* DIEGO) de los delitos de conspiración para cometer un delito de terrorismo y del delito de tenencia de explosivos por el que venían siendo acusados en este procedimiento, declarando de oficio otras seis diecinueveavas partes de las costas procesales causadas.

Que debemos CONDENAR y CONDENAMOS a Everardo como autor de un delito consumado de pertenencia a organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de diez años de prisión, con su accesoria de inhabilitación absoluta durante el tiempo de la condena y como autor de un delito de falsificación de documento público con finalidad terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de tres años de prisión y multa de doce meses con cuota diaria de 10 euros, lo que totaliza una pena de multa de 3.600 euros, con su accesoria de inhabilitación especial para el desempeño de todo empleo o cargo público durante el tiempo de la condena, así como al pago de dos de diecinueveavas partes de las costas procesales causadas en el procedimiento.

Que debemos CONDENAR y CONDENAMOS a JUAN CARLOS, *alias*Imanol como autor de un delito consumado de pertenencia a organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de diez años de prisión, con su accesoria de inhabilitación absoluta durante el tiempo de la condena y como autor de un delito de falsificación de documento público con finalidad terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de tres años de prisión y multa de doce meses con cuota diaria de 10 euros, lo que totaliza una pena de multa de 3.600 euros, con su accesoria de inhabilitación especial para el desempeño de todo empleo o cargo público durante el tiempo de la condena, así como al pago de dos diecinueveavas partes de las costas procesales causadas en este procedimiento.

Que debemos CONDENAR y CONDENAMOS a JOSÉ ANTONIO como autor de un delito consumado de pertenencia a organización terrorista, sin la concurrencia de circunstancias modificativas de las responsabilidad criminal a la pena de diez años de prisión, con su accesoria de inhabilitación absoluta durante el tiempo de la condena y como autor de un delito de falsificación de documento público con finalidad terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de tres años de prisión y multa de doce meses con cuota diaria de 10 euros, lo que totaliza una pena de multa de 3.600 euros, con su accesoria de inhabilitación especial para el desempeño de todo empleo o cargo público durante el tiempo de la condena, así como al pago de dos diecinueveavas partes de las costas procesales causadas en este procedimiento.

Que debemos CONDENAR y CONDENAMOS a MIGUEL como autor de un delito consumado de pertenencia a organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de diez años de prisión, con su accesoria de inhabilitación absoluta durante el tiempo de la condena y como autor de un delito de falsificación de documento público con finalidad terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de tres años de prisión y multa de doce meses con cuota diaria de 10 euros, lo que totaliza una pena de multa de 3.600 euros, con su accesoria de inhabilitación especial para el desempeño de todo empleo o cargo público durante el tiempo de la condena, así como al pago de dos diecinueveavas partes de las costas procesales causadas en este procedimiento.

Que debemos CONDENAR y CONDENAMOS a ÁNGEL *alias* Pitufo, *alias* DIEGO, como autor de un delito consumado de pertenencia a organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de diez años de prisión, con su accesoria de inhabilitación absoluta durante el tiempo de la condena y como autor de un delito de falsificación de documento público con finalidad terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de tres años de prisión y multa de doce meses con cuota diaria de 10 euros, lo que totaliza una pena de multa de 3.600 euros, con su accesoria de inhabilitación especial para el desempeño de todo empleo o cargo público durante el tiempo de la condena, así como al pago de dos diecinueveavas partes de las costas procesales causadas en este procedimiento. A todos ellos, además, expresamente se les condena al comiso de la totalidad de los bienes, objetos y efectos intervenidos. Y para el cumplimiento de la pena principal y responsabilidad personal subsidiaria que se les impone en esta resolución, les será de abono todo el tiempo que han estado privado de libertad por esta causa, si no lo tuvieran absorbido en otra. Notifíquese a las partes la presente resolución, haciéndoles saber que la misma no es firme y que contra ella cabe recurso de CASACIÓN por infracción de Ley o quebrantamiento de forma en el plazo de cinco días.

3.- Notificada la sentencia a las partes, se prepararon recursos de casación por infracción de preceptos constitucionales e infracción de ley, que se tuvieron por anunciados, remitiéndose a esta Sala Segunda del Tribunal Supremo las certificaciones necesarias para su sustanciación y resolución, formándose el rollo y formalizándose el recurso.

4.- El recurso interpuesto por EVERARDO se basó en los siguientes

MOTIVOS DE CASACIÓN:

Primero.-En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

Segundo.-Se renuncia.

Tercero.-Se renuncia.

Cuarto.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

Quinto.- En el quinto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

Sexto.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP.

Séptimo.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Octavo.- En el octavo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

El recurso interpuesto por *ÁNGEL* se basó en los siguientes MOTIVOS DE CASACIÓN:

Primero.-En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

Segundo.-Se renuncia.

Tercero.-Se renuncia.

Cuarto.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

Quinto.- En el quinto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías, en relación al principio acusatorio, que proclama el artículo 24.2 CE.

Sexto.- En el sexto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

Séptimo.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP.

Octavo.- En el octavo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Noveno.- En el noveno motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

El recurso interpuesto por JUAN CARLOS, se basó en los siguientes MOTIVOS DE CASACIÓN:

Primero.-En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

Segundo.-Se renuncia.

Tercero.-Se renuncia.

Cuarto.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

Quinto.- En el quinto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP.

Sexto.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Séptimo.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

El recurso interpuesto por JOSÉ ANTONIO se basó en los siguientes MOTIVOS DE CASACIÓN:

Primero.-En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

Segundo.-Se renuncia.

Tercero.-Se renuncia.

Cuarto.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

Quinto.- En el quinto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP.

Sexto.- En el sexto motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Séptimo.- En el séptimo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

El recurso interpuesto por MIGUEL se basó en los siguientes MOTIVOS DE CASACIÓN:

Primero.-En el primer motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a un proceso con todas las garantías que proclama el artículo 24.2 CE.

Segundo.-Se renuncia.

Tercero.-Se renuncia.

Cuarto.- En el cuarto motivo del recurso, formalizado al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 LECrim, se invoca vulneración del derecho a la presunción de inocencia que proclama el artículo 24.2 CE.

Quinto.- En el quinto motivo del recurso, formalizado al amparo del nº 2º del artículo 849 LECrim, se invoca error en la apreciación de la prueba basado en documentos que obran en autos que demuestran la equivocación del juzgador sin resultar contradichos por otros elementos probatorios.

Sexto.- En el sexto motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 574, 390 y 392 CP.

Séptimo.- En el séptimo motivo del recurso, formalizado al amparo del nº 1º del artículo 849 LECrim, se invoca infracción, por aplicación indebida, de los artículos 515.2 y 516.2 CP.

Octavo.- En el octavo motivo del recurso, formalizado al amparo del número 1º del artículo 849 LECrim, se invoca infracción del artículo 66.6 CP.

5.- Instruído el Ministerio Fiscal y demás partes de los recursos interpuestos, la Sala admitió los mismos, quedando conclusos los autos para señalamiento de vista cuando por turno correspondiera.

6.- Hecho el señalamiento para la vista, se celebró la misma y la votación prevenida el día 4 de octubre de 2007. Con fecha 15 de octubre de 2007 se dictó

auto de prórroga del plazo para dictar sentencia por quince días más.

DECISIÓN

Se estiman los recursos parcialmente y se dicta una nueva sentencia y se declaran de oficio las costas.

"DEBEMOS DECLARAR Y DECLARAMOS HABER LUGAR PARCIALMENTE A LOS RECURSOS DE CASACIÓN por infracción de preceptos constitucionales e infracción de Ley interpuestos:

Procede, en consecuencia, dejar sin efecto las condenas impuestas a los acusados JOSÉ ANTONIO y MIGUEL por el delito de falsedad con finalidad terrorista, absolviéndoles de este delito y declarándose de oficio la parte correspondiente de las costas. Asimismo, acorde con los razonamientos expresados en la primera sentencia de casación, procede sustituir las penas impuestas a los acusados EVERARDO, ÁNGEL, JUAN CARLOS, JOSÉ ANTONIO y MIGUEL, por el delito de pertenencia a organización terrorista, que lo fue de diez años de prisión, con la accesoria de inhabilitación absoluta durante el tiempo de la condena, a cada uno de ellos, por la de SEIS AÑOS DE PRISIÓN e inhabilitación especial para empleo o cargo público por tiempo de seis años, a cada uno de los acusados.

Respecto al delito de falsedad con finalidad terrorista, se sustituyen las penas impuestas a los acusados EVERARDO, ÁNGEL y JUAN CARLOS, de tres años de prisión y multa de doce meses, por la de UN AÑO Y NUEVE MESES DE PRISIÓN Y MULTA DE SEIS MESES, a cada uno de estos tres acusados, con la misma cuota diaria fijada en la sentencia de instancia".

RATIO DECIDENDI

De los recursos presentados se estiman:

- Recurso interpuesto por EDUARDO: Se estiman los motivos nº 1 y 8.
- Recurso interpuesto por ÁNGEL: Se estiman los motivos nº 1, 5 y 9.

- Recurso interpuesto por JUAN CARLOS: Se estiman los motivos nº 1 y 7.
- Recurso interpuesto por JOSÉ ANTONIO: Se estiman los motivos nº 1, 5 y 7.
- Recurso interpuesto por MIGUEL: Se estiman los motivos nº 1, 5, 6 y 8.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

ÚNICO.- Se aceptan y reproducen los fundamentos jurídicos de la sentencia recurrida a excepción de aquellos extremos que se pronuncian por la existencia de un delito de falsedad cometido por los acusados JOSÉ ANTONIO y MIGUEL que deben ser sustituidos por los correspondientes de la sentencia de casación en la que se declara la inexistencia de ese delito con relación a estos dos acusados; igualmente se modifican los razonamientos expresados para la fijación de las penas impuestas a los acusados que se sustituyen y complementan por los expresados en la sentencia de casación, al examinar el último de los motivos de todos los recurrentes.

Procede, en consecuencia, dejar sin efecto las condenas impuestas a los acusados JOSÉ ANTONIO y MIGUEL por el delito de falsedad con finalidad terrorista, absolviéndoles de este delito y declarándose de oficio la parte correspondiente de las costas.

Asimismo, acorde con los razonamientos expresados en la primera sentencia de casación, procede sustituir las penas impuestas a los acusados EVERARDO, ÁNGEL, JUAN CARLOS, JOSÉ ANTONIO y MIGUEL, por el delito de pertenencia a organización terrorista, que lo fue de diez años de prisión, con la accesoria de inhabilitación absoluta durante el tiempo de la condena, a cada uno de ellos, por la de SEIS AÑOS DE PRISIÓN e inhabilitación especial para empleo o cargo público por tiempo de seis años, a cada uno de los acusados.

Respecto al delito de falsedad con finalidad terrorista, se sustituyen las penas impuestas a los acusados EVERARDO, ÁNGEL y JUAN CARLOS, de tres años de prisión y multa de doce meses, por la de UN AÑO Y NUEVE MESES DE

PRISIÓN Y MULTA DE SEIS MESES, a cada uno de estos tres acusados, con la misma cuota diaria fijada en la sentencia de instancia.

Manteniendo y ratificando los restantes pronunciamientos de la sentencia anulada, procede absolver a JOSÉ ANTONIO y MIGUEL del delito de falsedad con finalidad terrorista de que fueron acusados, declarándose de oficio la parte correspondiente de las costas. Y procede sustituir las penas impuestas a los acusados EVERARDO, ÁNGEL, JUAN CARLOS, JOSÉ ANTONIO y MIGUEL por el delito de pertenencia a organización terrorista, que lo fue de diez años de prisión, con la accesoria de inhabilitación absoluta durante el tiempo de la condena, a cada uno de ellos, por la de SEIS AÑOS DE PRISIÓN e inhabilitación especial para empleo o cargo público por tiempo de seis años, a cada uno de los acusados. Y respecto al delito de falsedad con finalidad terrorista, procede sustituir las penas impuestas a los acusados EVERARDO, ÁNGEL y JUAN CARLOS, de tres años de prisión y multa de doce meses, por la de UN AÑO Y NUEVE MESES DE PRISIÓN Y MULTA DE SEIS MESES, a cada uno de estos tres acusados, con la misma cuota diaria fijada en la sentencia de instancia.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

V.3.- SENTENCIA 503/2008

V.3.1.- Análisis de la Sentencia

ROJ: STS 4587/2008 - ECLI:ES:TS:2008:4587
Nº Sentencia: 503/2008 Tipo Órgano: Tribunal Supremo. Sala de lo Penal. Municipio: Madrid -- Sección: 1. Resumen: Terrorismo de raíz islamista radical: atentados del 11-M en Madrid, perpetrados por miembros de la organización terrorista ¿Al Qaeda?

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	Vicente Pons Gamón
FECHA:	07-01-2007
PROYECTO:	"Ciberterrorismo, legislación: aplicación y seguridad"
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	STS 4587/2008
	Nº de Recurso: 10012/2008 Nº de Resolución: 503/2008
FECHA y LOCALIDAD.	MADRID – 17/07/200
PROCEDIMIENTO	Penal - apelación procedimiento abreviado
MAGISTRADO PONENTE:	D. Miguel ColmeneroMenéndez de Luarca
DEMÁS MAGISTRADOS	D. Juan Saavedra Ruiz D. Andrés Martínez Arrieta D. Juan Ramón Berdugo Gómez de la Torre D. Luciano Varela Castr
VOTO PARTICULAR:	NO SE REALIZA VOTO PARTICULAR

Ilustración 40: *STS 4587/2008.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. MIGUEL COLMENERO MENÉNDEZ DE LUARCA, demás magistrados D. JUAN SAAVEDRA RUIZ, D. ANDRÉS MARTÍNEZ ARRIETA, D. JUAN RAMÓN BERDUGO GÓMEZ DE LA TORRE y LUCIANO VARELA CASTRO, sin que se tenga constancia de voto particular (ilustración 40).

Terrorismo de raíz islamista radical: atentados del 11-M en Madrid, perpetrados por miembros de la organización terrorista Al Qaeda. El juicio de los atentados del 11 de marzo de 2004 es un proceso judicial de mucha trascendencia mediática ya que es el mayor juicio terrorista sufrido en territorio Español, que se llevó a cabo en Madrid en relación con los atentados del 11 de marzo de 2004. El juicio se celebró entre el 15 de febrero de 2007 y el 2 de julio de 2007, cuando el juicio quedó visto para sentencia. Hubo un total de 57 sesiones, que se celebraron en un pabellón de la Audiencia Nacional de España en la Casa de Campo. Se dictó sentencia el 31 de octubre de 2007 en la que se consideró probado que los atentados de Madrid, que causaron 191 muertos y 1.857 heridos, fueron llevados

a término por una célula yihadista, siete de cuyos miembros se suicidaron en Leganés el 3 de abril de 2004, más JAMAL ZOUGAM, OTHMAN EL GNAOUI y otro yihadista no identificado, con la cooperación necesaria del minero JOSÉ EMILIO SUÁREZ TRASHORRAS, quien facilitó el robo de los explosivos.

Los principales acusados del juicio eran: JAMAL ZOUGAM, ABDELMAJID BOUCHAR 'El Gamo', JOSÉ EMILIO SUÁREZ TRASHORRAS, RABEI OSMAN 'El Egipcio', HASSAN EL HASKI, YOUSSEF BELHADJ 'ABU DUJANAH', FOUAD EL MORABIT AMGHAR, BASEL GHALYOUN, MOUHANNAD ALMALLAH 'DABAS', MOHAMED LARBI BEN SELLAM 'ABU ZUBAIR', además de los acusados citados, hubo 19 más, hasta completar los 29 acusados del juicio.

El Tribunal Supremo el 17/07/2008, por las razones expuestas en sentencia de casación, procede absolver de los delitos a los acusados OSCAR, CARLOS ALBERTO, PAULINO y PEDRO.

Procede absolver al acusado FELIX del delito de falsedad en documento oficial.

Procede absolver al acusado ALEXANDER del delito de tráfico de drogas que causan grave daño a la salud, y procede condenarlo por delito de tráfico de drogas que no causan grave daño a la salud. No se le impondrá pena de multa en cuanto no se precisa en la sentencia el valor de la droga.

Procede condenar al acusado José como autor de un delito de pertenencia a organización terrorista a la pena de 9 años de prisión.

Procede condenar al acusado JUAN LUIS como autor de un delito de pertenencia a organización terrorista en grado de dirigente a la pena de 14 años de prisión.

Procede condenar a los acusados HUMBERTO y SERGIO como autores de un delito continuado de falsedad en documento oficial a la pena de dos años de prisión y multa de 10 meses con cuota diaria de 10 euros a cada uno de ellos.

Procede condenar al acusado LUIS MANUEL como autor de un delito de tráfico de explosivos a la pena de cuatro años de prisión.

Asimismo, procede rectificar las indemnizaciones acordadas en la sentencia en la forma que resulta de los fundamentos de esta Sentencia de casación, lo que se precisará en la medida necesaria en ejecución de sentencia[311].

V.3.2.- Aspectos de interés

NORMA DEMANDADA

Delitos de estragos terroristas, asesinatos terroristas y pertenencia o integración en organización terrorista islámica, tráfico de drogas, sustracción, traslado y entrega de sustancias explosivas empleadas en atentado terrorista.

PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNAL SUPREMO

Que debemos DECLARAR y DECLARAMOS HABER LUGAR a los recursos de casación interpuestos por los acusados OSCAR, CARLOS ALBERTO, PAULINO y PEDRO.

Que debemos DECLARAR y DECLARAMOS HABER LUGAR PARCIALMENTE a los recursos de casación interpuestos por los acusados FELIX, ALEXANDER, JOSÉ y JUAN LUIS.

Que debemos DECLARAR y DECLARAMOS HABER LUGAR PARCIALMENTE a los recursos de casación interpuestos por las acusaciones particulares en nombre de CONCEPCIÓN; ROSA y otros; ASOCIACIÓN 11-M AFECTADOS POR EL TERRORISMO Y ASOCIACIÓN AYUDA A LA VÍCTIMAS DEL 11-M Y OTROS.

Todos los anteriores recursos interpuestos contra la sentencia dictada por la Audiencia Nacional (Sala de lo Penal, Sección Primera), con fecha treinta y uno de octubre de dos mil siete, en causa seguida contra ROBERTO, CARLOS DANIEL, ALBERTO, GABINO, OSCAR, CARLOS ALBERTO, ALEXANDER, LUIS MANUEL, FELIX,

[311] Vid. STS, Sala de lo penal nº 503 de 17 de julio de 2008. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=1458813&links=&optimize=20081002&publicinterface=true

PAULINO, CARLOS ANTONIO, ALEJANDRO, FERNANDO, MÓNICA, LUIS, JUAN MARÍA, ENRIQUE, PEDRO, LUIS CARLOS, ARMANDO, HUMBERTO, SERGIO, JUAN LUIS, JESÚS CARLOS, MARCOS, CLEMENTE, JOSÉ, JOSÉ ÁNGEL y VICTOR MANUEL; casando la Sentencia de la Audiencia Nacional y procediendo a dictar nueva sentencia conforme a Derecho. Con declaración de oficio de las costas procesales correspondientes a estos recursos.

Que debemos DECLARAR y DECLARAMOS NO HABER LUGAR al recurso de casación interpuesto por el Ministerio Fiscal contra la sentencia dictada por la Audiencia Nacional (Sala de lo Penal, Sección Primera), con fecha treinta y uno de octubre de dos mil siete, en causa seguida contra ROBERTO, CARLOS DANIEL, ALBERTO, GABINO, OSCAR, CARLOS ALBERTO, ALEXANDER, LUIS MANUEL, FELIX, PAULINO, CARLOS ANTONIO, ALEJANDRO, FERNANDO, MÓNICA, LUIS, JUAN MARÍA, ENRIQUE, PEDRO, LUIS CARLOS, ARMANDO, HUMBERTO, SERGIO, JUAN LUIS, JESÚS CARLOS, MARCOS, CLEMENTE, JOSÉ, JOSÉ ÁNGEL y VICTOR MANUEL; con declaración de oficio de las costas procesales correspondientes a este recurso.

Que debemos DECLARAR y DECLARAMOS NO HABER LUGAR a los recursos interpuestos por los acusados ROBERTO; CARLOS DANIEL; ALBERTO; JOSÉÁNGEL; CARLOS ANTONIO; FERNANDO; GABINO; ALEJANDRO; LUIS CARLOS; ARMANDO; CLEMENTE, y VICTOR MANUEL.

Que debemos DECLARAR y DECLARAMOS NO HABER LUGAR a los recursos interpuestos por las acusaciones particulares en nombre de ARTURO; MILLÁN; GASPAR y LUIS PABLO y otros.

Todos los anteriores recursos interpuestos contra la sentencia dictada por la Audiencia Nacional (Sala de lo Penal, Sección Primera), con fecha treinta y uno de octubre de dos mil siete, en causa seguida contra ROBERTO, CARLOS DANIEL, ALBERTO, GABINO, OSCAR, CARLOS ALBERTO, ALEXANDER, LUIS MANUEL, FELIX, PAULINO, CARLOS ANTONIO, ALEJANDRO, FERNANDO, MÓNICA, LUIS, JUAN MARÍA, ENRIQUE, PEDRO, LUIS CARLOS, ARMANDO, HUMBERTO, SERGIO, JUAN LUIS, JESÚS CARLOS, MARCOS, CLEMENTE, JOSÉ, JOSÉ ÁNGEL y VICTOR MANUEL; fueron desestimados, condenándoles al pago de las costas ocasionadas por sus respectivos recursos.

Comuníquese esta resolución a la mencionada Audiencia a los efectos legales oportunos, con devolución de la causa que en su día remitió interesando acuse de recibo.

Así por esta nuestra sentencia que se publicará en la Colección Legislativa, lo pronunciamos, mandamos y firmamos.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

Terrorismo. Organización terrorista. Concepto. Pertenencia. Grado de dirigente. Mera expresión de ideas. Realización de actividades demostrativas del paso a la acción. Descripción fáctica suficiente. Grupos o células integradas en otra organización.

Grupos o células independientes. Posibilidad de pertenencia a varias organizaciones terroristas.

Terrorismo de raíz islamista radical.

Derechos fundamentales. Restricciones en casos de delitos graves.

Necesidad de una motivación suficiente.

Secreto de las comunicaciones telefónicas.

Inviolabilidad del domicilio. Secreto del sumario.

Exigencias para garantizar la inexistencia de indefensión.

Posibilidad de instruirse de la causa y proponer diligencias.

Presunción de inocencia.

Reconocimientos fotográficos.

Reconocimientos en rueda. Declaraciones testificales.

Declaraciones de coimputados: requisitos para su valoración. Posibilidad de contradicción. Inmediación.

Testimonios de referencia. Valor de las diligencias practicadas en otros

países.

Control de legalidad. Prueba indiciaria. Exclusión de inferencias excesivamente abiertas o inconsistentes.

Error en la apreciación de la prueba. Particular del documento acreditativo del error. No autoriza a rectificar la valoración del conjunto de la prueba.

Cooperación necesaria. *Dolo* eventual en el cooperador. Doctrina de la Sala Segunda del Tribunal Supremo.

Conocimiento del efecto de la aportación respecto del peligro concreto de realización del tipo por el autor.

Complicidad.

Tráfico de explosivos. Con organización terrorista.

Con conocimiento de su probable utilización en hechos concretos. *Dolo* eventual, motivación de las sentencias, individualización de la pena, gravedad de los hechos resultante del relato fáctico.

Tutela judicial efectiva.

La resolución motivada satisface el derecho aunque sea equivocada, si no es arbitraria. Posible vulneración de otros derechos.

Sentencia absolutoria. Las dudas sobre la corrección de la absolución no conducen directamente a la condena. Prohibición de *bis in idem.* Fundamento. Efectos en el ámbito interno y en el internacional. Normas internas. Normas internacionales.

Determinación de la jurisdicción. Decisión de no proceder. Efectos. Sentencia firme. Posibilidad reducida de un segundo enjuiciamiento y una segunda condena.

Normas Jurídicas.

- El recurso interpuesto por EL MINISTERIO FISCAL se basó en los siguientes MOTIVOS DE CASACIÓN: Por infracción de Ley al amparo del

nº 1 del art. 849 LECrim por inaplicación indebida de los arts. 515.2 y 516.2 CP, en relación con el 666.2 LECrim.

- El recurso interpuesto por la representación de la ASOCIACIÓN 11-M AFECTADOS POR EL TERRORISMO (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 849. Vulneración del artículo 25.1 de la CE en relación con el artículo 24 del mismo texto constitucional. Vulneración del artículo 24.1 y 2 de la CE. Inaplicación indebida de los artículos 572.1. Vulneración del artículo 25.1 y 24. Inaplicación del artículo 572.1.1º CP; 571.1.1º. Inaplicación del artículo 568 CP.

- El recurso interpuesto por la representación de la ASOCIACIÓN DE AYUDA A LAS VÍCTIMAS DEL 11-M Y OTROS (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Por infracción de precepto constitucional al amparo del artículo 852 LECrim y 5.4 de la Ley Orgánica del Poder Judicial. Por errores en la apreciación de diferentes pruebas, al amparo del artículo 849.2 LECrim.

- El recurso interpuesto por la representación de MILLÁN (Acusación Particular) se basó en el siguiente MOTIVO DE CASACIÓN: Al amparo de lo dispuesto en el artículo 849 por aplicación indebida del artículo 115 CP y la doctrina jurisprudencial que lo desarrolla.

- El recurso interpuesto por la representación del recurrente ROSA, BENITO Y DIANA, REPRESENTANTES LEGALES DE MARÍA CONSUELO (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del artículo 851.1 LECrim y 852. Vulneración del art. 24 CE. Al amparo del art. 849,1 y.2.Infracción de Ley por inaplicación del artículo 572.1.Infracción de Ley por inaplicación del artículo 568 CP.Vulneración del artículo 24.1 y 2 de la CE. Vulneración del artículo 25.1 y 24. Inaplicación del art. 516.1º CP.

- El recurso interpuesto por la representación del recurrente LUIS PABLO, MARIBEL, LUIS MIGUEL, YOLANDA, DOMINGO, JUAN RAMÓN, MIGUEL ÁNGEL y LUIS ANDRÉS (Acusación Particular) se basó en los siguientes MOTIVOS DE

CASACIÓN: Motivo al amparo del art. 849.1 y 2 LECrim. Aplicación indebida del artículo 115 CP.

- El recurso interpuesto por la representación del recurrente ARTURO (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de ley, conforme previene el artículo 849.1.Infracción de ley al amparo del artículo 849.1.No aplicación del artículo 572.1.1º.Infracción del artículo 849.1. Al amparo de lo establecido en los artículos 852 LECrim y 5.4 de la Ley Orgánica del Poder Judicial. Al amparo de los artículos 852 LECrim y 5.4 de la Ley Orgánica del Poder Judicial.Vulneración los artículos 24 (tutela judicial efectiva) y 25 (principio de legalidad) CE.

- El recurso interpuesto por la representación del recurrente Concepción (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 849.1. y 2 Inaplicación indebida de preceptos penales, art. 573. Inaplicación del art. 57. Inaplicación artículos 568 y 573 CP. Aplicación indebida del artículo 25 CE. Vulneración del Derecho Constituciónal a la Presunción de Inocencia del art. 24 CE.

- El recurso interpuesto por la representación del recurrente Gaspar (Acusación Particular) se basó en los siguientes MOTIVOS DE CASACIÓN: Por vulneración del art. 849 de la LEC por la existencia de error en la apreciación de la prueba.

- El recurso interpuesto por la representación del recurrente ROBERTO (condenado) se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 5.4 de la Ley Orgánica del Poder Judicial y del art. 852 LECrim.

- El recurso interpuesto por la representación del recurrente CARLOS Daniel se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de Ley (art. 849.1 LECrim). Infracción de Ley con base en el art. 849.1 LECrim.Infracción art. 571, 346 CP, 572.1.1º del CP, 144 CP y 392 CP.Quebrantamiento de forma del art. 851.1 LECrim.Infringidos los arts. 20.1, 21.1, 21.6, 66 y el art. 72 CP.

- El recurso interpuesto por la representación del recurrente ALBERTO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de ley (error de Derecho) conforme artículo 849.1 y 2 LECrim.Indebida aplicación artículo 573 CP. Indebida inaplicación de artículo 579.3 CP.Indebida inaplicación de artículos 21.4 y 21.5 Código Penal.Quebrantamiento de Forma por Vicios *in procediendo*, conforme 850.1 LECrim. Quebrantamiento de Forma *(vicios in iudicando)* conforme artículo 851.1 y 3 LECrim. Por vulneración de precepto Constituciónal conforme artículo 852 LECrim artículos 24.1 y 2 CE.

- El recurso interpuesto por la representación del recurrente GABINO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de ley del art. 24.1 y 24.2. Artículos 515.2 y 516.2 CP. Art. 849.2. Art. 851.1.

- El recurso interpuesto por la representación del recurrente ÓSCAR se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del punto 4 del artículo 5 de la Ley Orgánica del Poder Judicial.Por infracción de preceptos constitucionales, en concreto de los artículos 2, 14, 16, 18 y 24.1de la CE.Al amparo del nº 1 del artículo 849.Infracción del artículo 120, 302, 320, 326, 330, 332, 334, 335, 459, LECrim.Artículos 515.2 y 516.2 CP. Al amparo del número 2 del artículo 849 de la Ley Procesal. Al amparo del artículo 850 de la Ley Procesal en sus puntos 1, 3 y 4. Al amparo del artículo 851 LECriminal en sus números 1 y 3.

- El recurso interpuesto por la representación del recurrente CARLOS ALBERTO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de precepto constitucional al amparo del art. 5.4 de la Ley Orgánica del Poder Judicial por infracción del art. 24 CE.Infracción de ley al amparo del art. 849.2. Al amparo del art. 5.4 de la LOPJ por vulneración del art. 24.1 de la Carta Magna.Al amparo del art. 849.1º LECrim.

- El recurso interpuesto por la representación del recurrente ALEXANDER se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de precepto constitucional, al amparo del art. 5.4 de la LOPJ. Infracción de Ley del artículo 849, 1. Infracción de lo dispuesto en los artículos 18.2 y 24.1 de la CE.Infracción de Ley, al amparo del art. 849.1. Aplicado indebidamente los

arts. 368 y 369 CP. Aplicación indebida de los arts. 515 y 516 del CP. Artículo 24.2.

- El recurso interpuesto por la representación del recurrente FÉLIX se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de precepto constitucional, al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y 852 LECrim.Por infracción de Ley, al amparo del número 1º del art. 849 LECrim.Por Infracción de ley, al amparo del nº 1º del art. 849 LECrim.Por Infracción de Ley, al amparo del nº 1º del art. 849 LECrim, por indebida aplicación del artículo 390.1 y 392 del CP. Por infracción de Ley, al amparo del nº 1º del art. 849 LECrim, por indebida aplicación del artículo 568 del CP.

- El recurso interpuesto por la representación del recurrente Paulino se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de Ley del artículo 849.1 y 2.Infracción de lo dispuesto en los artículos 18.2 y 24.1 CE. Infracción de Ley del art. 11.1 LOPJ. Vulneración del art. 24 CE. Infracción del artículo 5.4º de la Ley Orgánica del Poder Judicial. Vulneración del art. 66 CP.

- El recurso interpuesto por la representación del recurrente CARLOS ANTONIO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de precepto constitucional. Infringido los arts. 14, 24 y 25 de la CE. Infracción del art. 849.1º LECrim. Por infracción de Ley al amparo del art. 849.1y 2 LECrim. Inaplicación de los art. 515.2º, 516.1º, 573, 568 y 458 del CP. Se infringe el art. 851. 1º, 2º y 3º LECrim.

- El recurso interpuesto por la representación del recurrente ALEJANDRO se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial. Aplicación indebida del artículo 515.2 CP. Aplicación indebida del artículo 516.2 CP.

- El recurso interpuesto por la representación del recurrente FERNANDO se basó en los siguientes MOTIVOS DE CASACIÓN: Vulneración de los artículos 515 y 516 del CP. El art. 66 del Código. Mal aplicación del art. 850. 1º, 2º, 3º y 4º. Mal aplicación del art. 851. Por infracción de precepto

constitucional (art. 5.4 LOPJ. y arts. 9, 10, 14, 17, 18 y 24 CE).

- El recurso interpuesto por la representación del recurrente PEDRO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción del artículo 849.1. Infracción del art.852 LECrim. Infracción del artículo 852 LECrim.Infracción del artículo 849.2 LECrim. Infracción de Ley que previene y autoriza el artículo 849.1 LECrim, al haberse aplicado indebidamente el artículo 66 del CP. Infracción de Ley que previene y autoriza el artículo 849.1 LECrim. Aplicación indebida el artículo 568 del CP.

- El recurso interpuesto por la representación del recurrente LUIS CARLOS se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del artículo 851 LECrim. Al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial. Vulneración del artículo 242 de la CE. Artículo 24.1 y 2 de la CE. Infracción del artículo 849.1 y 2 LECrim.

- El recurso interpuesto por la representación del recurrente ARMANDO se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 851.1 LECrim. Al amparo del art. 5.4 de la Ley Orgánica del Poder Judicial.Infracción del art. 849.1 LECrim. Infracción del artículo 849.1 y 2 LECrim.

- El recurso interpuesto por la representación del recurrente HUMBERTO se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 5.4 de la Ley Orgánica del Poder Judicial al haberse infringido el art. 24.2 de la CE.Infracción del artículo 849.1 y 2 LECrim.Indebida aplicación del art. 392 y 74.1 CP.

- El recurso interpuesto por la representación del recurrente SERGIO se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción del art. 852, 847, 851 y artículo 5,4 de la Ley Orgánica del Poder Judicial. Principio de legalidad (art. 9.3 y 25 CE). Incongruencia de la sentencia. (Art. 24.2 CE). Infracción del artículo 849.1 LECrim. Indebida aplicación arts. 392 CP, 390.1, 239 y 240 LECrim. Indebida aplicación del art. 851, 3 LECrim.

- El recurso interpuesto por la representación del recurrente JUAN LUIS se

basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del artículo 849.1 y 2 LECrim. Aplicación indebida de los artículos 515.2º y 516.1º CP.

- El recurso interpuesto por la representación del recurrente CLEMENTE se basó en los siguientes MOTIVOS DE CASACIÓN: Al amparo del art. 5.4 de la Ley Orgánica del Poder Judicial y del art. 852 LECrim. Al amparo de lo previsto en el art. 11.1 LOPJ y 852 LECrim.Por infracción de precepto constitucional por el cauce del art. 5.4 de la Ley Orgánica del Poder Judicial y 852 LECrim. Infracción de Ley, al amparo de lo establecido en el art. 849.1 LECrim, por infracción del artículo 66.6 CP.

- El recurso interpuesto por la representación del recurrente JOSÉ se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción de art. 24.2 Presunción de inocencia. Al amparo del art. 5.4 de la LOPJ y art. 852 LECrim, por infracción del art. 24.1 y 2 CE. Al amparo del art. 851.1 LECrim. Al amparo del art. 849.1 LECrim.

- El recurso interpuesto por la representación del recurrente JOSÉ ÁNGEL se basó en los siguientes MOTIVOS DE CASACIÓN Inaplicación del art. 24 de la CE. Artículo 518 CP. Se aplica inadecuadamente el párrafo 2 del art. 515 del CP.Aplicación indebida del artículo 568 CP art. 24 de CE.

- El recurso interpuesto por la representación del recurrente VICTOR MANUEL se basó en los siguientes MOTIVOS DE CASACIÓN: Infracción del artículo 852 LECrim y el art. 5.4 de la LOPJ. Vulneración art. 24 CE.

- Instruidas las partes recurridas, los impugnaron respectivamente; habiéndose solicitado la celebración de Vista y quedando conclusos los autos para señalamiento de Vista cuando por turno correspondiera.

- Hecho el señalamiento para Vista, se celebró la misma los días treinta de junio, 1 y 2 de Julio de dos mil ocho. Habiéndose celebrado igualmente la deliberación hasta el día de hoy.

DEMANDA

El **juicio de los atentados del 11 de marzo de 2004** es el proceso judicial que se llevó a cabo en Madrid en relación con los atentados del 11 de marzo de 2004. El juicio se celebró entre el 15 de febrero de 2007 y el 2 de julio de 2007, cuando el juicio quedó visto para sentencia. Hubo un total de 57 sesiones, que se celebraron en un pabellón de la Audiencia Nacional de España en la Casa de Campo. Se dictó sentencia el 31 de octubre de 2007 en la que se consideró probado que los atentados de Madrid, que causaron 191 muertos y 1.857 heridos, fueron llevados a término por una célula yihadista, siete de cuyos miembros se suicidaron en Leganés el 3 de abril de 2004, más JAMAL ZOUGAM, OTHMAN EL GNAOUIy otro yihadista no identificado, con la cooperación necesaria del minero JOSÉ EMILIO SUÁREZ TRASHORRAS, quien facilitó el robo de los explosivos.

Los principales acusados del juicio eran:

- JAMAL ZOUGAM.
- ABDELMAJID BOUCHAR 'El Gamo'.
- JOSÉ EMILIO SUÁREZ TRASHORRAS.
- RABEI OSMAN 'El Egipcio'.
- HASSAN EL HASKI.
- YOUSSEF BELHADJ 'Abu Dujanah'.
- FOUAD EL MORABIT AMGHAR.
- BASEL GHALYOUN.
- MOUHANNAD ALMALLAH 'Dabas'.
- MOHAMED LARBI BEN SELLAM 'Abu Zubair'.

Además de los acusados citados anteriormente, hubo 19 más, hasta completar los 29 acusados del juicio.

La sentencia determina, como hechos probados:

1. En relación al origen de los explosivos, la participación en su robo y destino del material robado por SUÁREZ TRASHORRAS, *El Chino*, ABDENNABI KOUNJAA y MOHAMED OULAD AKCHA, que *«toda o gran parte de la dinamita de los artefactos que explosionaron en los trenes del 11 de marzo y toda la que fue detonada en el piso de Leganés procedía de la mina Conchita... Entre octubre de 2003 y enero de 2004, JAMAL AMIDHAN acordó con TRASHORRAS el*

suministro de dinamita procedente de las minas asturianas... y TRASHORRAS hizo llegar los días 5 y 9 de enero dos cargamentos de explosivos desde Asturias a Madrid... La dinamita era sustraída de mina Conchita... El 28 de febrero de 2004, SUÁREZ TRASHORRAS junto a JAMAL AHMIDÁN, fue a recoger a MONTOYA VIDAL en el Toyota Corolla. En otro vehículo iban los fallecidos MOHAMED OULAD AKCHA y ABDENNABI KOUNJAA. Ambos vehículos se dirigían hacia la mina... Una vez allí, SUÁREZ y El Chino se adentraron en ella [la mina]... y regresaron y TRASHORRAS le comentó a JAMAL AHMIDAN que se acordara de coger las puntas y tornillos... Se dirigieron a Avilés, donde compraron tres mochilas... regresando a la mina [con ellas] y regresaron con las mochilas cargadas... y en Avilés descargaron los explosivos de las mochilas. Seguidamente volvieron a la mina por tercera vez y repitieron la operación para regresar cargados... El 29 de febrero, El Chino, MOHAMED OULAD AKCHA y KOUNJAA emprendieron viaje de vuelta a Madrid con los explosivos».

2. La Fiscalía, la Asociación 11-M Afectados del Terrorismo, la Asociación de Ayuda a las Víctimas del 11-M, varias víctimas particulares y los ventinueve acusados presentaron recursos de casación ante el Tribunal Supremo contra la sentencia de la Audiencia Nacional. Los de los acusados iban dirigidos a la absolución; los de la Fiscalía y los afectados a incrementar las penas de algunos condenados y obtener la condena de algunos acusados que habían sido absueltos.

3. En sentencia del 17 de julio de 2008, el Tribunal Supremo mantuvo, en líneas generales, las condenas establecidas por la Audiencia Nacional, absolviendo a tres condenados y condenando a uno de los juzgados exonerados.

4. De la resolución, en lo que se refiere a las condenas, el Supremo mantuvo la absolución de RABEI OSMAN EL SAYED, que lo había sido por considerarse que por el delito de integración en banda armada u organización terrorista que se consideraba probado, ya había sido condenado en Italia; absolvió además a MOUHANNAD ALMALLAH, ABDELILAH FADUAL EL AKIL y RAÚL GONZÁLEZ PELÁEZ por falta de pruebas y condenó a cuatro años de prisión a Antonio Toro por un delito de tráfico de explosivos, por el que había sido absuelto en la

Audiencia. Aplicó también modificación de condenas a: OTHMAN EL GNAOUI, por considerarlo inocente del delito de falsedad de documentos públicos, aunque aumentó la pena total por autor material del atentado; Hamid Ahmidan, le condenó a doce años de prisión pero se le quitó la multa por tráfico de drogas y a HASSAN EL HASKI se le ajustó la pena de 15 años de prisión a 14, por ser éste el límite previsto en el Código Penal para el delito de integración en banda armada.

DECISIÓN

SENTENCIA

En la Villa de Madrid, a diecisiete de Julio de dos mil ocho.

En la causa número 10012/2008 del Juzgado Central de Instrucción número seis de Madrid, seguida por delitos de estragos terroristas, asesinatos terroristas y pertenencia o integración en organización terrorista islámica, tráfico de drogas, sustracción, traslado y entrega de sustancias explosivas empleadas en atentado terrorista, contra ROBERTO, con N.I.E. 242, hijo de MOHAMED y de ELENA, nacido en Tanger (Marruecos) el 5/10/1973; CARLOS DANIEL, con D.N.I. nº. 243, hijo de JOSÉ MANUEL y AGRIPINA, nacido en Avilés (Asturias) el 10/12/1976; ALBERTO, con N.I.E. 244, hijo de AZZID y AMINA, nacido en Casablanca (Marruecos) el 15/06/1979; GABINO, con N.I.E. 245, hijo de MOHAMED y ELGHALIA, nacido en Nador (Marruecos) el 3/09/1975; ÓSCAR, con N.I.E. 246, hijo de WALID y WAFA, nacido en Homs (Siria) el 25/02/1980; CARLOS ALBERTO, con N.I.E.247, hijo de MOHAMMAD y IBTISSAM, nacido en Damasco (Siria) el 25/02/1964; ALEXANDER, con pasaporte nº. 248, hijo de FADEL y NFADLA, nacido en Tetuán (Marruecos) el 20/11/1977; LUIS MANUEL, con D.N.I. nº. 249, hijo de VICTORIANO y MARÍA DEL CARMEN, nacido en Avilés (Asturias) el 13/07/1977; FÉLIX, con pasaporte nº. 073, hijo de MOHAMED y de FÁTIMA, nacido en Tetuán (Marruecos) el 25/04/1975; PAULINO, con N.I.E. 250, hijo de MOHAMED y FÁTIMA, nacido en Tetuán (Marruecos) el 26/10/1969; CARLOS ANTONIO, con N.I.E. 251, hijo de MOHAMED y FÁTIMA, nacido en Kouribga (Marruecos) el 19/11/1.979; ALEJANDRO, con N.I.E. 252, hijo de ABDESLAM y RHIMOU, nacido en Tánger (Marruecos) el 11/05/1.979; FERNANDO, con N.I.E. 253, hijo de ABDELAZIZ y de ZOHRA, nacido en BENI GUERFET (Marruecos) el 10/04/1.973;

MÓNICA, con D.N.I. nº. 254, hija de MARÍA CARMEN y VICTORINO, nacida en Avilés (Asturias) el 17/08/1.981; LUIS, con D.N.I. nº. 255, hijo de MANUEL y VICTORIA, nacido en Avilés (Asturias) el 23/08/1.982; JUAN MARÍA, con D.N.I. nº. 256, nacido en Avilés (Asturias); ENRIQUE, con D.N.I. nº. 257, hijo de AVELINO y de OLVIDO, nacido en Cangas del Narcea (Asturias) el 15/12/1.960; PEDRO, con D.N.I. nº. 258, hijo de JOSÉ y MARÍA TERESA, nacido en Oviedo (Asturias) el 28/07/1.979; LUIS CARLOS, con D.N.I. nº. 259, hijo de JOSÉMANUEL y ELIÉCER MARÍA JESÚS, nacido en Avilés (Asturias) el 9/05/1.981; ARMANDO, con D.N.I. nº. 260, hijo de PILAR y JOAQUÍN, nacido en Oviedo (Asturias) el 23/08/1.982; HUMBERTO, con N.I.E.261, hijo de SALA y ALGIA, nacido en CONSTANTINA (Argelia) el 19/05/1.961; Sergio, hijo de nº. 262 y SIENA, nacido en Beirut (Líbano) en el año 1960; JUAN LUIS, con pasaporte nº.098 hijo de MOHAMMAD y de MHIJIBA, nacido en Guelmin (Marruecos) el 5/08/1.963; JESÚSCARLOS, con N.I.E. 263, hijo de ALLAL y de SAFIA, nacido en Rhababa Taza (Marruecos) el 12/11/1.983; MARCOS, con N.I.E. 264, hijo de ALLAL y de SAFIA, nacido en Khababa (Marruecos), el 25/09/1.984; CLEMENTE, con pasaporte número –nº. 265, hijo de AHMED y de AICH, nacido en B. Touzine (Marruecos) el 27/05/1.976; JOSÉ, con N.I.E. nº. 266, hijo de AICHA y de ABDESLAM, nacido en Tánger (Marruecos) el 10/06/1.977; JOSÉ ÁNGEL, nacido en Ait Lahcen Oualla (Marruecos) el 9/01/1.983; y VICTOR MANUEL, con N.I.E. nº. 267, hijo de nº. 268 y de nº. 269, nacido en Gharbia (Egipto) el 22/07/1971; la Audiencia Nacional dictó sentencia con fecha treinta y uno de octubre de dos mil siete, que ha sido CASADA Y ANULADA PARCIALMENTE por lo que los Excmos. Sres. Magistrados anotados al margen, bajo la Presidencia del primero de los indicados y Ponencia del Excmo. Sr. D. MIGUEL COLMENERO MENÉNDEZ DE LUARCA, proceden a dictar esta Segunda Sentencia con arreglo a los siguientes:

I. ANTECEDENTES

Único.- Se reproducen e integran en esta Sentencia todos los de la sentencia de instancia, salvo en la medida en que resultan afectados por la sentencia de casación.

III. FALLO

QUE DEBEMOS CONDENAR Y CONDENAMOS:

Al acusado JUAN LUIS como autor de un delito de pertenencia a organización terrorista en grado de dirigente a la pena de 14 años de prisión e inhabilitación especial para empleo o cargo público por tiempo de 15 años.

Al acusado JOSÉ, como autor de un delito de pertenencia a organización terrorista en grado de integrante, a la pena de 9 años de prisión e inhabilitación especial para empleo o cargo público por tiempo de 10 años.

A los acusados HUMBERTO y SERGIO como autores de un delito de falsedad en documento oficial a la pena de 2 años de prisión y multa de 10 meses con cuota diaria de 10 euros. Con responsabilidad personal subsidiaria en caso de impago de la multa. Y accesoria de inhabilitación especial para el derecho de sufragio pasivo durante el tempo de la condena.

Al acusado ALEXANDER como autor de un delito de pertenencia a organización terrorista a la pena de 12 años de prisión, con la accesoria de inhabilitación especial para empleo o cargo público por 14 años y como autor de un delito de tráfico de drogas que no causan grave daño a la salud a la pena de un año de prisión, y accesoria de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena, absolviéndole del delito de tráfico de drogas por el que venía condenado.

QUE DEBEMOS ABSOLVER Y ABSOLVEMOS al acusado FÉLIX del delito de falsedad en documento oficial, manteniendo la condena por los demás delitos.

QUE DEBEMOS ABSOLVER Y ABSOLVEMOS a los acusados ÓSCAR y CARLOS ALBERTO del delito de pertenencia a organización terrorista.

QUE DEBEMOS ABSOLVER Y ABSOLVEMOS al acusado PAULINO del delito de colaboración con organización terrorista.

QUE DEBEMOS ABSOLVER Y ABSOLVEMOS al acusado PEDRO del delito de tráfico de explosivos.

En cuanto a las responsabilidades civiles se acuerda fijar el importe del depósito que se constituye a favor de MARÍA CONSUELO en la cantidad de 500.000 euros, manteniendo las demás cantidades acordadas en la sentencia.

Se acuerda incluir al recurrente Inocencio entre las víctimas de los atentados del 11 de marzo, determinándose la inclusión en el grupo que corresponda y el importe de la indemnización en ejecución de sentencia teniendo en cuenta los datos ya obrantes en la causa y los criterios establecidos en la sentencia de instancia.

Se incrementa la indemnización del lesionado JOSÉ AUGUSTO en 100 euros por cada día de los 52 que reclama hasta la intervención quirúrgica para corregir la segunda perforación timpánica.

Se acuerda incluir a los lesionados nº. 235, nº. 236 y nº. 237 en el Grupo 3.

Se acuerda incluir a los lesionados nº. 238, nº. 239 y nº. 241 en el Grupo 4.

Se acuerda incluir a la lesionada nº. 240 en el Grupo 6.

Se mantienen los demás pronunciamientos de la sentencia de instancia no afectados por la presente.

Así por esta nuestra sentencia, que se publicará en la Colección Legislativa, lo pronunciamos, mandamos y firmamos.

JUAN SAAVEDRA RUIZ, ANDRÉS MARTÍNEZ ARRIETA, MIGUEL COLMENERO MENÉNDEZ DE LUARCA.

JUAN RAMÓN BERDUGO GÓMEZ DE LA TORRE, LUCIANO VARELA CASTRO.

PUBLICACIÓN.- Leídas y publicadas han sido las anteriores sentencias por el Magistrado Ponente Excmo. Sr. D. MIGUEL COLMENERO MENÉNDEZ DE LUARCA, mientras se celebraba audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Secretario certifico.

RATIO DECIDENDI (rd) "la razón de la decisión"

ÚNICO.- Por las razones expuestas en nuestra sentencia de casación procede absolver de los delitos por los que venían condenados a los acusados OSCAR; CARLOS ALBERTO; PAULINO y PEDRO.

Procede asimismo, absolver al acusado FÉLIX del delito de falsedad en documento oficial.

Procede absolver al acusado ALEXANDER del delito de tráfico de drogas que causan grave daño a la salud, y procede condenarlo por delito de tráfico de drogas que no causan grave daño a la salud. No se le impondrá pena de multa en cuanto no se precisa en la sentencia el valor de la droga.

Procede condenar al acusado JOSÉ como autor de un delito de pertenencia a organización terrorista a la pena de 9 años de prisión.

Procede condenar al acusado JUAN LUIS como autor de un delito de pertenencia a organización terrorista en grado de dirigente a la pena de 14 años de prisión.

Procede condenar a los acusados HUMBERTO y SERGIO como autores de un delito continuado de falsedad en documento oficial a la pena de dos años de prisión y multa de 10 meses con cuota diaria de 10 euros a cada uno de ellos.

Procede condenar al acusado LUIS MANUEL como autor de un delito de tráfico de explosivos a la pena de cuatro años de prisión.

Asimismo, procede rectificar las indemnizaciones acordadas en la sentencia en la forma que resulta de los fundamentos de esta Sentencia de casación, lo que se precisará en la medida necesaria en ejecución de sentencia.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

El Tribunal Supremo dictó la sentencia “definitiva” sobre la matanza del 11-M, cuatro años y cuatro meses después de la tragedia. A lo largo de 959 páginas confirmó los elementos esenciales con los que la Audiencia Nacional explicó en octubre de 2007 el atentado más salvaje de la historia de España y ratificó una condena de más de 120.000 años de cárcel, la mayor impuesta en este país, para los principales autores vivos de la masacre y sus colaboradores. Para el Supremo no cabe duda de que el atentado en el que murieron 191 ciudadanos y otros 1.857 resultaron heridos fue obra de un comando islamista «con dependencia ideológica

de Al-Qaeda», y que ETA no tuvo participación alguna en la masacre. Pese a ratificar la esencia de la primera sentencia, una estricta aplicación del delito de pertenencia a organización terrorista y de la presunción de inocencia llevó al alto tribunal a absolver a cuatro de los 29 condenados, al tiempo que confirmó la libertad de RABEI OSMÁN, 'El Egipcio', no porque ya estuviese condenado en Italia por hecho similares, como defendió la Audiencia Nacional, sino por no encontrar pruebas suficientes para encarcelarlo por estos hechos. El Supremo sólo anula una de las siete absoluciones de la Audiencia Nacional, la de ANTONIO TORO, al que condena a cuatro años por tráfico de explosivos, muy lejos de los 34.715 años impuestos a su ex cuñado, EMILIO SUÁREZ TRASHORRAS, por proporcionar a los terroristas la dinamita con la que pudieron volar los cuatro trenes de cercanías. Según el tribunal, sólo hay pruebas de que TORO colaboró en la fase inicial, cuando no se sabía cuál era el posible destino del explosivo. La sala reafirma que un grupo 'yihadista', fiel a las directrices de Al-Qaeda pero sin dependencias jerárquicas o financieras conocidas, comenzó a preparar en 2003 los atentados de las estaciones de Atocha, Santa Eugenia y El Pozo. La célula liderada por SERHANE BEN FAKHET, 'El Tunecino', muerto días después de la masacre en la explosión del piso franco de Leganés, colocó en los cuatro trenes trece mochilas con unos 140 kilos de explosivos, la mayor parte robados por la red de SUÁREZ TRASHORRAS en Mina Conchita. El comando lo formaban entre 10 y 13 personas. El Supremo ratificó la condena a más de 42.900 años de cárcel a los dos únicos autores materiales vivos y detenidos, OTHMÁN EL GNAOUI y JAMAL ZOUGAM. El tribunal señala que les acompañaron en los trenes buena parte de los siete fallecidos en Leganés, un individuo no identificado, dos de los huidos muertos en 2005 en Irak- y, quizás, el procesado y aún no juzgado ABDELILLAH HRIZ. El grupo operativo, según la sentencia ratificada, estaba respaldado por una célula terrorista formada, al menos, por otros ocho de los condenados que contaba con dos colaboradores directos y la ayuda ocasional de tres traficantes de explosivos y dos falsificadores. Los 18 seguirán en la cárcel. El Supremo destaca en la sentencia el gran trabajo realizado por las fuerzas de seguridad y la justicia de España, que se ha convertido en el único país del mundo en lograr capturar, juzgar y condenar con todas las garantías a la mayor parte de los implicados vivos en un gran atentado internacional.

«Pasar a la acción»

El alto tribunal, que dictó la resolución en un tiempo récord de siete meses, rechazó el recurso de la Fiscalía y las impugnaciones de la mayor parte de las acusaciones particulares, y aprovechó para fijar una clara doctrina sobre la definición de una organización terrorista islamista: no hace falta que una organización extremista cometa delitos violentos o haya iniciado la fase final de un atentado; lo fundamental es que se pueda acreditar que sus miembros «han pasado del pensamiento a la acción» para realizar sus fines «mediante la violencia o el terror». Asimismo, advierte de que no basta con probar que un radical contacta con otros radicales, sino que «hay que probar que ha decidido pasar a la acción». «La coincidencia ideológica con otras personas, aunque sea en ideas violentas, y la relación entre ellos no acredita por sí misma la pertenencia a organización terrorista», resume la tesis. Esta doctrina es la que lleva al tribunal a absolver a BASEL GHALYOUN, MOUHANNAH ALMALLAH y FADUAL EL AKIL, que ya han sido excarcelados. La corte admite que se trata de personas radicales, que mantenían contacto con otros extremistas y conocían a miembros del grupo terrorista, pero concluye que no hay pruebas suficientes de que hubiesen «pasado a la acción». El cuarto absuelto es el ex minero asturiano RAÚL GONZÁLEZ, 'el Rulo'. La sala considera que no existen pruebas de que ayudó a Suárez Trashorras en el robo y tráfico de explosivos.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

V.4.- SENTENCIA 363/2012

V.4.1.- Análisis de la Sentencia

ROJ: STS 3123/2012 - ECLI:ES:TS:2012:3123
Nº Sentencia: 363/2012 **Tipo Órgano: Tribunal Supremo. Sala de lo Penal** **Municipio: Madrid -- Sección: 1** **Resumen: Principio acusatorio. Presunción de inocencia. Pertenencia a organización terrorista.**

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	**Vicente Pons Gamón**
FECHA:	**07-01-2007**
PROYECTO:	**"Ciberterrorismo, legislación: aplicación y seguridad"**
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	**STS 3123/2012 - ECLI: ES:TS:2012:3123**
	Nº de Recurso: 11268/2011 **Nº de Resolución: 363/2012**
FECHA y LOCALIDAD.	**MADRID – 09/05/2012SALA SEGUNDA DE LO PENAL**
PROCEDIMIENTO	**Penal procedimiento abreviado/sumario**
MAGISTRADO PONENTE:	**JOSÉ MANUEL MAZA MARTÍN**
DEMÁS MAGISTRADOS	**D. Cándido Conde Pumpido Tourón** **D. Julián Sánchez Melgar** **D. José Manuel Maza Martín** **D. Manuel Marchena Gómez**
VOTO PARTICULAR:	**No hay voto particular**

Ilustración 41: *STS 3123/2012 - ECLI: ES: TS: 2012:3123.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. JOSÉ MANUEL MAZA MARTÍN, demás magistrados D. CÁNDIDO CONDE PUMPIDO TOURÓN, D. JULIÁN SÁNCHEZ MELGAR, D. MANUEL MARCHENA GÓMEZy ALBERTO JORGE BARREIRO (ilustración 41), sin que se tenga constancia de voto particular.

Los acusados son juzgados, por pertenencia a banda armada, tenencia de útiles para falsificar documentos y difusión del Islam con terroristas buscados por la justicia española, a través de medios violentos, tal como enseña la *yihad* islámica, integrándose en una red ya existente y cuyo objeto era ayudar a huir a terroristas facilitándoles todos los medios posibles, disponiendo de un inmueble que servía de alojamiento para algunos elementos de la red y labores de ocultamiento indicadas.

El Juzgado Central de Instrucción número 6 con el número 49/2009 y seguida ante la Audiencia Nacional, Sala de lo Penal, Sección Cuarta, lleva causa contra cinco acusados por delitos de integración en organización terrorista y tenencia de útiles para la falsificación de documentos, dictando sentencia el 15 de abril del 2015 en la cual se absuelve a dos de ellos y se acusa a otros de pertenencia a organización terrorista condenando a uno de ellos a 10 años de cárcel, costas e inhabilitación y al otro a seis años de cárcel, costas e inhabilitación al quinto por un delito de tenencia de útiles para la falsificación de documentos oficiales a la pena 2 años de prisión, costas y multa de 6 meses. La Sentencia de instancia fue casada y anulada parcialmente por la pronunciada por la Sala Segunda del Tribunal Supremo y que se resume en:

Absolver a un acusado, del delito de integración en organización terrorista del que venía siendo acusado en estas actuaciones, con todos los pronunciamientos favorables y declaración de oficio de las costas procesales causadas en la instancia y a él atribuibles, manteniendo el resto de pronunciamientos condenatorios contenidos en la Resolución de instancia respecto de los otros dos acusados[312].

V.4.2.- Aspectos de interés

NORMA DEMANDADA

- Integración en organización terrorista de carácter islamista.
- Envío de fondos a otros miembros de la organización ubicados en el extranjero.
- Delito de tenencia de útiles para la falsificación documental.

PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNALSUPREMO

[312] Vid. STS, Sala de lo penal nº 363 de 9 de mayo de 2012. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=6386450&links=&optimize=20120529&publicinterface=true

Exaltación de actividades terroristas. Elemento subjetivo del tipo. Inferencia. Justificaciones inaceptables y no armonizables con los hechos objetivos reconocidos por el acusado.

Pretendida justificación con el ejercicio de derechos constitucionales [art. 20.1. a) y b)]. Rebasamiento de los límites de estos derechos.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

El recurso interpuesto por REMIGIO:

Primero.- Por infracción de precepto constitucional, al amparo del art. 5. 4º de la LOPJ, al haberse infringido el art. 24 de la CE en relación con el principio de presunción de inocencia.

Segundo.- Por infracción de ley, al amparo del art. 849. 2º LECrim, por error en la valoración de la prueba.

Tercero.- Por infracción de ley, al amparo del art. 849. 2º LECrim, al haberse infringido en la sentencia los arts. 390. 1º, 392, 400 y 574 CP.

El recurso interpuesto por ROGELIO:

Primero.- Por infracción del art. 24.1 y 2 de la CE, al entender que se ha lesionado el derecho a la presunción de inocencia. Se formula al amparo del art. 5. 4º de la LOPJ y del art. 53. 1 y 2 del texto constitucional.

Segundo.- Por vulneración del principio acusatorio constitucionalmente consagrado en los derechos de tutela judicial y no indefensión, a ser informado de la acusación y un proceso con todas las garantías; conforme regula el art. 24 de la CE, por vía del art. 5. 4º de la LOPJ y art. 852 LECrim.

Tercero.- Por infracción de ley, al amparo del art. 849. 2º LECrim, al haberse incurrido en error en la apreciación de la prueba, basado en documentos que obran en autos.

Cuarto.- Por infracción de ley, al amparo del art. 849. 1º LECrim, por infracción de precepto penal sustantivo, en concreto, por aplicación indebida de

los artículos 515.2º y 516 CP, derogados por la L.O. 5/2010 y, con ellos, aplicación indebida, del delito tipificado en el art. 571, tras la nueva redacción dada al precepto, en virtud de la L.O. 5/2010, vulnerándose por inaplicación del art. 2.2 CP, el principio de retroactividad de la Ley Penal favorable.

Quinto.- Por quebrantamiento de forma, al amparo del art. 851. 1º LECrim, al haberse consignado en los Hechos probados de la sentencia recurrida, expresiones conceptuales, de naturaleza técnico-jurídica que implican la predeterminación del fallo y han sido conducentes a la condena.

El recurso interpuesto por ROQUE:

Primero.-Por quebrantamiento de forma, al amparo del art. 851 LECrim.

Segundo.-Por infracción de ley, al amparo del art. 849. 1º LECrim, por aplicación indebida del art. 571.2º CP.

Tercero.-Al amparo del art. 5. 4º de la LOPJ, por infracción del art. 24. 2º de la CE, y al amparo del art. 849. 1º LECrim, por infracción de la presunción de inocencia.

DEMANDA

PRIMERO.- ROGELIO, mayor de edad y sin antecedentes penales, conociendo la comisión de los atentados de Madrid del 11 de marzo de 2.004, sabiendo que, entre otros, habían participado: LUIS FRANCISCO, *alia*s, “Chipirón”; JUAN MIGUEL, *alias*, “Ratón”; ADOLFO, quien también era llamado “Gamba”, “Corsario”, o “Mangatoros”; DIONISIO;EMILIANO y EVELIO, (según se deduce de la sentencia nº 31/2009, de 30 de abril, dictada por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional en la llamada operación “Tigris” y confirmada en casación en la sentencia nº 10931/2009 P de 21/12/2009) con quien compartía la difusión del Islam a través de medios violentos tal como enseña la yihad islámica, sabiendo que eran buscados por la justicia española, se integró en una red ya existente-y de la que ya se habla en las referidas resoluciones- cuyo objeto era ayudar a huir a los citados.De otra, tener a su disposición un inmueble que, aún en condiciones precarias, servía de alojamiento tanto para algunos elementos

de la red, como para las labores de ocultamiento indicadas.

SEGUNDO.- La vivienda, a la que sus ocupantes llamaban “Al Kalaa” (fortaleza), se encontraba en la CALLE 000 nº.000 de Santa Coloma de Gramanet (Barcelona), desempeñaba una doble misión, de una parte, era la residencia habitual de personas con ideología radical islamista, y de otra, y como consecuencia de ello, albergaba o daba cobijo a personas perseguidas por la justicia.Habían decidido abandonarla y dar su vida en Irak, como radicales islamistas que previamente adoctrinados estaban dispuestos a hacer “*la yihad*” en Irak contra los infieles, constituyendo, en ambos casos, el último eslabón de residencia en España.

TERCERO.- El denominado tercer apoyo de la red, estaba formado por la colaboración de personas ajenas a los acusados pero conformes a la ideología defendida por los integrantes de la red, gracias a cuya colaboración algunos de los huidos solventaron sus problemas de carencia de pasaportes o documentación necesaria para pasar de un país a otro.

CUARTO.- ROGELIO, mayor de edad y sin antecedentes penales, persona de toda confianza de la red, era el encargado de remitir cantidades de dinero a personas que habiendo conseguido huir de España, necesitaban colaboración económica hasta llegar a su destino que no era otro que hacer “*la yihad*”en Irak; de esta manera, y como ya ocurriera con Salvador, (integrante de la misma red y condenado en la denominada operación “Tigris”, por el envío a determinados huidos de diversas cantidades de dinero, a la pena de 9 años de prisión en sentencia firme) envió dinero a través de diversas oficinas de la *Western Unión* de Santa Coloma de Gramanet (Barcelona).

QUINTO.- ROQUE, mayor de edad y sin antecedentes penales, tuvo una antigua y prolongada relación de amistad con ADOLFO, (que utilizaba los nombres de Corsario, Gótico, Topo, Cojo, Gamba u Zanagollas), quien, como ya se ha indicado, tras ser identificado por poner una de las mochilas en los trenes que explotaron el 11 de marzo de 2.004, y ocultado por la red, en la “*Al kalaa*”, emprendió huida con dirección a Irak para llevar a cabo la “Yihad”, y adonde consiguió llegar gracias a la obtención de un pasaporte marroquí falso facilitado por IVÁN en Estambul (tal como resulta de los datos obrantes en las dos

Comisiones Rogatorias practicadas en relación al citadoIVÁN con Argelia y de la sentencia condenatoria dictada por las autoridades argelinas) llegando a ostentar en Irak un papel importante en la estructura de Al Qaeda identificado con el nombre de Ildefonso.

SEXTO.- REMIGIO, mayor de edad y sin antecedentes penales, aparece en las presentes actuaciones como consecuencia de su relación con VÍCTOR a quien conocía antes del 2004, y quien como ya se ha dicho, huyó de España después del 11 de marzo, llegando en su periplo hacia Irak, hasta Estambul, desde donde llamó a REMIGIO a su teléfono nº. 007 para pedirle 100 euros que no le fueron enviados y donde tras conseguir un pasaporte falso gracias a la intervención de IVÁN, (según consta en las Comisiones rogatorias ya indicadas), a quien le facilitó el teléfono de REMIGIO, regresó a Barcelona, entrevistándose con el citado REMIGIO con el que tomó un café, trasladándose posteriormente VÍCTOR a la *"Al kalaa"* donde fue detenido el 15 de junio de 2.004 y posteriormente juzgado y condenado en la llamada operación "Tigris" como integrante en organización terrorista.

SÉPTIMO.- PEDRO MIGUEL, mayor de edad y sin antecedentes penales, conoció a dos personas relacionadas con las investigaciones realizadas en torno al atentado del 11 de marzo de 2.004 y suicidios producidos en la vivienda sita en la CALLE 003 nº. 001 de Leganés, el suicidado ARTURO, *alias* "Moro" y otro huido de la justicia española, el ciudadano marroquí DIONISIO.

DECISIÓN

FALLO. Que debemos declarar y declaramos haber lugar a la desestimación de los Recursos de Casación interpuestos por las Representaciones de ROGELIO y ELOISA contra la Sentencia dictada por la Sección Cuarta de la Sala de lo Penal de la Audiencia Nacional, el 15 de Abril de 2010, por delitos de integración en organización terrorista y tenencia de útiles para la falsificación de documentos oficiales, a la vez que estimamos íntegramente el Recurso interpuesto por la Representación de ROQUE contra esa misma Resolución, debiéndose dictar a continuación la correspondiente Segunda Sentencia. Se declaran de oficio las costas procesales ocasionadas por el Recurso que se estima, imponiendo a los otros dos recurrentes las causadas por los suyos.

Póngase en conocimiento del Tribunal de origen, a los efectos legales oportunos, la presente Resolución y la que seguidamente se dictará, con devolución de la Causa que, en su día, nos fue remitida. Así por esta nuestra sentencia que se publicará en la Colección Legislativa, lo pronunciamos, mandamos y firmamos CÁNDIDO CONDE PUMPIDO TOURÓN, JULIÁN SÁNCHEZ MELGAR, JOSÉ MANUEL MAZA MARTÍN, MANUEL MARCHENA GÓMEZ, ALBERTO JORGE BARREIRO, 11268/2011P, Ponente Excmo. Sr. D.JOSÉ MANUEL MAZA MARTÍN. Vista: 26/04/2012. Secretaría de Sala: Ilmo. Sr. D. JUAN ANTONIO RICO FERNÁNDEZ TRIBUNAL SUPREMO Sala de lo Penal.

SEGUNDA SENTENCIA nº: 363/2012 Excmos. Sres: D. CÁNDIDO CONDE PUMPIDO TOURÓN, D. JULIÁN SÁNCHEZ MELGAR, D. JOSÉ MANUEL MAZA MARTÍN, D. MANUEL MARCHENA GÓMEZ, D. ALBERTO JORGE BARREIRO. En nombre del Rey, La Sala Segunda de lo Penal, del Tribunal Supremo, constituída por los Excmos. Sres. mencionados al margen, en el ejercicio de la potestad jurisdiccional que la Constitución y el pueblo español le otorgan, ha dictado la siguiente SENTENCIA:

En la Villa de Madrid, a nueve de mayo de dos mil doce. En la causa incoada por el Juzgado Central de Instrucción nº 6 con el nº 49/2009 y seguida ante la Audiencia Nacional, Sala de lo Penal, Sección Cuarta, por delitos de integración en organización terrorista y tenencia de útiles para la falsificación de documentos, contra ROGELIO con N.I.E. nº. 018, nacido el nº. 019 de 1985, en Ksar Kebir (Marruecos), hijo de AHMED y de ANISA, contra REMIGIO con N.I.E. nº. 020, nacido el nº. 021 de 1977, en Cebala (Túnez), hijo de LLAIDD y de BACHRA, contra ROQUE con N.I.E. nº. 022, nacido el nº. 023 de 1964, en Mohammadia (Argelia), hijo de MOHAMED y de FATMA y contra PEDRO MIGUEL con N.I.E. nº. 024, nacido el nº. 025 de 1974, en Casablanca (Marruecos), hijo de MUSTAPHA y de ALDA, en cuya causa se dictó sentencia por la mencionada Audiencia con fecha 15 de abril de 2011, que ha sido casada y anulada parcialmente por la pronunciada en el día de hoy por esta Sala Segunda del Tribunal Supremo, integrada por los Excmos. Sres. expresados al margen y bajo la Ponencia del Excmo. Sr. D. JOSÉ MANUEL MAZA MARTÍN, hace constar lo siguiente:

I. ANTECEDENTES. ÚNICO.- Se aceptan y reproducen los antecedentes de Hecho y los fundamentos fácticos de la sentencia dictada por la Audiencia

Nacional, Sala de lo Penal, Sección Cuarta.

II. FUNDAMENTOS DE DERECHO. PRIMERO.- Se tienen aquí por reproducidos los fundamentos de nuestra anterior Sentencia de Casación, así como los de la recurrida, en lo que no se opongan a los primeros. SEGUNDO.- Como ya se ha dicho en el Fundamento Jurídico Quinto de los de la Resolución que precede, sin necesidad de alterar el relato de hechos probados de la Sentencia de la Audiencia, procede la absolución del acusado Roque por la ausencia de carácter punible de la conducta que en el *"factum"* de la Resolución de la Audiencia se le atribuye. En su consecuencia, vistos los preceptos mencionados y demás de general aplicación al caso.

III. FALLO. Que debemos absolver y absolvemos al acusado, ROQUE, del delito de integración en organización terrorista del que venía siendo acusado en las presentes actuaciones, con todos los pronunciamientos favorables y declaración de oficio de las costas procesales causadas en la instancia y a él atribuibles, manteniendo el resto de pronunciamientos condenatorios contenidos en la Resolución de instancia respecto de los otros dos acusados. Así por esta nuestra sentencia, que se publicará en la Colección Legislativa, lo pronunciamos, mandamos y firmamos CÁNDIDO CONDE PUMPIDO TOURÓN, JULIÁN SÁNCHEZ MELGAR, JOSÉ MANUEL MAZA MARTÍN, MANUEL MARCHENA GÓMEZ, ALBERTO JORGE BARREIRO.

PUBLICACIÓN.- Leidas y publicadas han sido las anteriores sentencias por el Magistrado Ponente Excmo. Sr. D. JOSÉ MANUEL MAZA MARTÍN, mientras se celebraba audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Secretario certifico.

La sentencia de instancia dictó el siguiente pronunciamiento: FALLAMOS: QUE DEBEMOS ABSOLVER Y ABSOLVEMOS a Pedro Miguel de los delitos por los que ha sido acusado, declarando de oficio una cuarta parte de las costas. QUE DEBEMOS ABSOLVER Y ABSOLVEMOS a ELOISA del delito de pertenencia a organización terrorista, declarando de oficio la parte proporcional de las costas. QUE DEBEMOS CONDENAR Y CONDENAMOS a ROGELIO y ROQUE como autores criminalmente responsables de un delito de integración en organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad

criminal a las penas siguientes: A ROGELIO, 10 añosde prisión e inhabilitación especial para empleo o cargo público durante 10 años y pago proporcional de las costas. AROQUE, 6 años de prisión e inhabilitación especial para empleo o cargo público durante 7 años y pago proporcional de las costas. QUE DEBEMOS CONDENAR Y CONDENAMOS a REMIGIO, como autor criminalmente responsable de un delito de tenencia de útiles para la falsificación de documentos oficiales a la pena de 2 años de prisión y multa de 6 meses a razón de 6 euros diarios y pago proporcional de las costas.

ARGUMENTO DE LA DECISIÓN
PROBLEMA JURÍDICO RESUELTO POR LA SENTENCIA

El recurrente en el primero de los dos motivos que alega, considera vulnerado el art. 24 CE en sus apartados 1º y 2º (tutela judicial efectiva y presunción de inocencia), aunque solo desarrolla y de forma muy escueta el último de los derechos fundamentales reseñados, protesta que canaliza a través del art. 5.4 LOPJ.

Con sede procesal en el art. 849.1º LECrim en relación al art. 20.1. A) y b) de la CE, por considerar que estaba ejercitando derechos fundamentales.Se les condena en base al art. 579.1, par. 2º del CP.

RATIO DECIDENDI (rd) “la razón de la decisión”

A) RECURSO DE ROGELIO:

1) El recurrente, condenado por el Tribunal de instancia, como autor de un delito de integración en organización terrorista, a la pena de diez años de prisión, fundamenta su Recurso de Casación en cinco diferentes motivos, de los que el Quinto de ellos, último ordinal de dicho Recurso pero primero por el que hemos de comenzar nuestro análisis dada su naturaleza formal, se refiere, con cita del artículo 851.1 LECrim, a la existencia en la narración fáctica que sirve de soporte a la recurrida de expresiones que, predeterminándolo, condicionan el fallo de la misma, al afirmar que el recurrente“... se integró en una red ya existente”, lo que supondría dar por supuesta esa “integración”. (Desestimado).

2) Por su parte, los dos primeros motivos, con cita de los artículos 5.4 de la Ley Orgánica del Poder Judicial y 852 LECrim, se refieren a sendas vulneraciones de derechos fundamentales, como la del derecho a la presunción de inocencia (art. 24.2 CE) y del derecho a un proceso con garantías, relacionado con el principio acusatorio y el derecho a ser debidamente informado de la acusación.

- En cuanto a la primera de tales supuestas infracciones, como sabemos, la tarea encomendada a este Tribunal de Casación, en orden a la debida tutela del derecho a la presunción de inocencia del recurrente, tan sólo nos obliga, además de a ejercer el oportuno control respecto de la validez de las pruebas de que se sirve la Resolución recurrida, extremo que ni plantea problema alguno ni tan siquiera ha sido cuestionado en el caso presente, a examinar la racionalidad de esa valoración y, en concreto, la adecuada correspondencia entre lo que se afirma como probado y los elementos en que dicha afirmación se funda.

- En tanto que por lo que se refiere a la otra de las vulneraciones denunciadas, es decir, la del derecho a un proceso con garantías, por no haber sido suficientemente informado de la acusación, al ser condenado como autor de un delito del vigente artículo 571 CP, cuando el Fiscal, en su escrito de Acusación, hacía referencia al artículo 515.2, en relación con el 516.2 coetáneos al tiempo de los hechos, lo que supondría además un incumplimiento del principio acusatorio, rector de nuestro sistema de enjuiciamiento penal, tales alegaciones han de ser rechazadas, toda vez que si examinamos los contenidos de los preceptos objeto de acusación y los aplicados en la condena no existe diferencia alguna entre unos y otros (Desestimado).

3) El tercer motivo del Recurso, versa, con cita del artículo 849.2º LECrim, sobre supuestos errores de hecho en los que habrían incurrido los Jueces *"a quibus"* a la hora de valorar la prueba documental obrante en las actuaciones y, en concreto, la pericial caligráfica en la que no pudo afirmarse que las firmas contenidas en los envíos dinerarios fueran de la autoría de ROGELIO (Desestimado).

4) Por su parte, en el Cuarto motivo del Recurso se cuestiona la aplicación del derecho sustantivo a los hechos declarados como probados (art. 849.1º LECrim), afirmando lo incorrecto de dicha aplicación en lo que se refiere al artículo 571.2 CP (o 515.2 º y 516.2º CP en su redacción anterior), es decir, el que contempla el supuesto delictivo de integración en organización terrorista (Desestimado).

B) RECURSO de ROQUE:

Este recurrente, condenado en los mismos términos que el anterior, si bien castigado con una pena de seis años de prisión, plantea su Recurso con apoyo en tres diferentes motivos, de los que procediendo el rechazo del Primero, relativo al quebrantamiento de forma consistente en la inclusión en el relato de hechos de la recurrida de expresiones predeterminantes del Fallo (art. 851.1 LECrim) con idénticos argumentos a los ya expuestos en el Fundamento Jurídico Primero de esta misma Resolución, destino desestimatorio que ha de compartir también el motivo Tercero, referente a la denuncia de vulneración del derecho a la presunción de inocencia (art. 5.4 LOPJ en relación al 24.2 CE), al existir prueba sobrada de lo narrado en el *"factum"* de la recurrida respecto de este recurrente, hemos de centrarnos en el examen del motivo Segundo del Recurso, relativo a la infracción de Ley en la que habría incurrido la Audiencia (art. 849.1º LECrim), al calificar la conducta descrita del recurrente como constitutiva de un delito de integración en organización terrorista. Y a este respecto hay que comenzar manifestando que, en efecto, le asiste toda la razón a ROQUE en su afirmación de que los hechos que se le atribuyen no integran infracción penal alguna, puesto que si examinamos tales datos fácticos nos encontramos con que los mismos consisten esencialmente en lo siguiente:

- Que mantenía una antigua amistad, desde hace aproximadamente veinte años con uno de los implicados en el atentado terrorista acaecido en Madrid el 11 de marzo de 2004.

- Que mantuvo el contacto con éste tras aquel luctuoso acontecimiento, incluso cuando abandonó nuestro país, conversando con él y manifestando la admiración que le profesaba por encarnar la lucha por sus ideales

religiosos.

- Que vendió un inmueble que poseía en España y se trasladó con su esposa, seguidamente, a su Argelia originaria, desconociéndose el destino que hubiera podido dar al dinero obtenido con la referida venta.

- Que entregó, en una ocasión, 500 euros a un tal YAHYA, ignorándose la causa de dicha entrega y su finalidad.

- Que recibió, cuando aún permanecía en nuestra nación, una llamada de su hermano desde Argelia, en la que éste le comunicó que la Policía de aquel país se había interesado por su paradero y que le recomendaba el regreso para que efectuase las correspondientes aclaraciones a los agentes policiales.

- Que en su domicilio se encontraron documentos relativos a dos teléfonos móviles. Evidentemente, el hecho de conocer, profesar amistad, compartir ideario en forma meramente teórica y mantener contactos y conversaciones con un miembro de una organización terrorista, sin ninguna otra forma de participación o colaboración con ésta, de carácter material y eficaz, no puede, en ningún caso, considerarse, como hizo la Audiencia en su Sentencia, como una forma de integración en dicha organización, o red, ni tan siquiera un supuesto de colaboración, también contemplado, como punible, en nuestro Código Penal, conclusión que tampoco permiten el resto de datos fácticos relativos a este recurrente que se describen en los hechos declarados como probados en la recurrida y que se acaban de enumerar sucintamente. Por lo que procede la estimación de este motivo y, con ella, la del Recurso, debiendo dictarse, a continuación, la correspondiente Segunda Sentencia en la que se declare la conclusión absolutoria derivada de semejante pronunciamiento estimatorio. (Estimado).

C) RECURSO de REMIGIO:

Por su parte, el tercer recurrente, condenado como autor de un delito de tenencia de útiles para la falsificación de documentos oficiales, a las penas dos años de prisión y multa, plantea tres motivos en su Recurso que pasamos a analizar en

forma individualizada:

1) Así, el Primero de tales motivos se refiere a la vulneración del derecho a la presunción de inocencia (art. 5.4 LOPJ en relación con el 24.2 CE), por falta de prueba suficiente para sustentar el pronunciamiento condenatorio en lo que a este recurrente respecta.

2) Por su parte, el motivo Segundo, con cita del artículo 849.2º LECrim, vuelve a hacer alusión a la misma cuestión que se acaba de abordar, aunque en esta ocasión alegando un supuesto error de hechos cometido por la Audiencia a la hora de valorar la prueba disponible en relación con el informe relativo a los útiles ocupados, en el que no se aportan los contrastes de los mismos con los originales de los sellos auténticos cuyo uso futuro falsario se atribuye al recurrente.

3) Mientras que por lo que se refiere, finalmente, a la supuesta infracción de Ley (art. 849.1º LECrim) cometido por la Audiencia al haber aplicado indebidamente los artículos 390.1, 392 y 400 CP, que describen el delito objeto de condena, semejante pretensión tampoco resulta sostenible, a la vista del contenido del *"factum"* de la recurrida a este respecto, con su carácter de intangibilidad (vid. FJ 4º de esta misma Resolución), en el que se describe un hecho que integra todos los elementos del delito de tenencia de útiles para la falsificación documental que tan correctamente se atribuye a NASREDDINE (Desestimado).

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

A) Recurso de ROGELIO:

- La narración fáctica del recurso tiene expresiones que, condicionan el fallo de la misma, al afirmar que el recurrente "se integró en una red ya existente", lo que supondría dar por supuesta esa "integración".

- Respecto al recurso sobre la presunción de inocencia, tan sólo nos obliga a ejercer el oportuno control respecto de la validez de las pruebas, y ni el propio recurrente en el recurso pone en duda esto.

- Proceso con garantías: los contenidos de los preceptos objeto de acusación y los aplicados en la condena no existe diferencia alguna entre unos y otros.

- Prueba caligráfica realizada con garantías.

- Con respecto a los hechos declarados probados el mismo recurso contempla el supuesto delictivo de integración en organización terrorista.

B) Recurso de ROQUE:

- En lo referente a la denuncia de vulneración del derecho a la presunción de inocencia existe prueba sobrada de lo narrado en el "factum".

- El resto de datos fácticos relativos a este recurrente sobre su pertenencia a banda armada que se describen en los hechos declarados enumerados no son suficientes para condenarlo. Por lo que procede la estimación de este motivo.

C) Recurso de REMIGIO:

- Valoración de la prueba correcta, no se aportan los contrastes de los mismos con los originales de los sellos auténticos.

- Se describe un hecho que integra todos los elementos del delito de tenencia de útiles para la falsificación documental.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

V.5.- SENTENCIA 114/2014

V.5.1.- Análisis de la Sentencia

ROJ: STS 474/2014 - ECLI:ES:TS:2014:474
Nº Sentencia: 114/2014 **Tipo Órgano: Tribunal Supremo. Sala de lo Penal** **Municipio: Madrid -- Sección: 1** **Resumen: Provocación para cometer actos terroristas.**

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	**Vicente Pons Gamón**
FECHA:	**07-01-2007**
PROYECTO:	**"Ciberterrorismo, legislación: aplicación y seguridad"**
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	**STS 474/2014 - ECLI:ES:TS:2014:474**
	Nº de Recurso: 1774/201 **Nº de Resolución: 114/2014**
FECHA y LOCALIDAD.	**MADRID – 20-02-2014**
PROCEDIMIENTO	**Penal procedimiento abreviado/sumario**
MAGISTRADO PONENTE:	**D. José Ramón Soriano Soriano**
DEMÁS MAGISTRADOS	**D. Cándido Conde Pumpido Tourón** **D. Julián Sánchez Melgar** **D. Alberto Jorge Barreiro** **D. Perfecto Andrés Ibáñez**
VOTO PARTICULAR:	**No hay voto particular**

Ilustración 42: *STS 474/2014 - ECLI: ES: TS: 2014:474.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. JOSÉ RAMÓN SORIANO SORIANO, demás magistrados D. CÁNDIDO CONDE PUMPIDO TOURÓN, D. JULIÁN SÁNCHEZ MELGAR, D. PERFECTO ANDRÉS IBÁÑEZ y ALBERTO JORGE BARREIRO (ilustración 42), sin que se tenga constancia de voto particular.

El acusado fue detenido porque administraba una web llamada "*Shabaka Al Haqiqa Al Ikhbaria"* traducido "red de la verdad informativa", no era una web de participación, se utilizaba para descargas, donde el acusado como administrador colgaba imágenes, vídeos y noticias respecto de temas yihadistas, incluidos vídeos de acciones terroristas o de Al Qaeda. Estas pretendían ser contrainformativas, y dar su versión desde el punto de vista radical yihadista.

El Juzgado Central de Instrucción nº 3 instruyó sumario con el nº 9 de 2012 contra el acusado, una vez concluso, lo remitió a la Sección Segunda Sala Penal

de la Audiencia Nacional, que con fecha 12 de julio de 2013 dictó sentencia en causa seguida contra él mismo por delito de pertenencia a organización terrorista y difusión del terrorismo en la que se le condena a 2 años de cárcel y 10 años de inhabilitación pública.

El fallo del Tribunal Supremo ratificó la sentencia de la Audiencia Nacional declarando no haber lugar a recurso de Casación por lo que además de confirmar la condena de 2 años de cárcel y 10 años de inhabilitación pública se le condena a las costas procesales derivadas de este recurso[313].

V.5.2.- Aspectos de interés

NORMA DEMANDADA
APOLOGÍA DEL TERRORISMO
PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNALSUPREMO

Exaltación de actividades terroristas. Elemento subjetivo del tipo. Inferencia. Justificaciones inaceptables y no armonizables con los hechos objetivos reconocidos por el acusado.

Pretendida justificación con el ejercicio de derechos constitucionales [art. 20.1. a) y b)]. Rebasamiento de los límites de estos derechos.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

Los preceptos constitucionales citados predican la libertad de expresión por cualquier medio, bien sea oral o escrito, con el único límite de los derechos de los demás y el honor y la propia imagen.

Al art. 579.1, par. 2º del CP que castigala distribución o difusión pública por cualquier medio de mensajes o consignas dirigidas a provocar, alentar o favorecer

[313] Vid. STS, Sala de lo penal nº 114 de 20 de febrero de 2014. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=6969757&links=&optimize=20140224&publicinterface=true

la perpetración de cualquiera de los delitos previstos en este capítulo (terrorismo).

La doctrina seguida por el TC. Así pues no se encontrarían bajo protección constitucional la realización de actos o actividades que, en el desarrollo de ciertas ideologías, vulneren otros derechos fundamentales.

DEMANDA

1.- El Juzgado Central de Instrucción nº 3 instruyó sumario con el nº 9 de 2012 contra JAIME, una vez concluso, lo remitió a la Sección Segunda Sala Penal Audiencia Nacional, que con fecha 12 de julio de 2013 dictó sentencia que contiene los siguientes Hechos Probados:

Primero.- El acusado JAIME mantenía y ha mantenido con posterioridad al 12 de julio de 2011 una intensa actividad como usuario en foros yihadistas radicales que operan en Internet, en concreto en los denominados "*Al Shumukh Al Islam*", "*Ansar Al Mujahideen*" y "*Al fidaa*", en los que albergaba con frecuencia posts, en línea y contenido con los que son frecuentes en dichos foros radicales. Tanto en el foro "Al Shumukh Al Islam", como "Ansar Al Mujahideen" se difunden con frecuencia comunicados y vídeos elaborados por organizaciones terroristas de carácter yihadista, o relacionados con actividades violento-terroristas realizadas por estas organizaciones. Son igualmente empleados con frecuencia como medio, no sólo de difusión de ideas o consignas, sino también para el adoctrinamiento, mútuo reforzamiento y autoafirmación de planteamientos radicales yihadistas de sus usuarios, y en ocasiones de plataforma para la captación y reclutamiento de personas interesadas en la comisión de hechos delictivos de carácter terrorista. El encausado, entraba en dichos foros utilizando como nombre de usuario el de "JUAN IGNACIO", y una clave, sin que exista absoluta constancia de que esta identidad virtual o *nickname* fuera utilizada únicamente por él con anterioridad al 12 de julio de 2011, que es a partir de cuándo se tiene plena constancia de su utilización por el acusado, como consecuencia de la monitorización de su linea ADSL, con autorización judicial, por parte de la policía. Los atributos que tenía concedidos y con los que firmaba el usuario "JUAN IGNACIO" en el foro eran los de "*shamlkh* el incitador" y "alumno de la facultad de aprendizaje de *Shumkh al Islam*".

Segundo.- En concreto el procesado, con la identidad "JUAN IGNACIO" colocó varios posts en el foro "*Al Shumukh Al Islam*" con la firma digital visual que había confeccionado (archivo en formato GIF en movimiento con varios fotogramas superpuestos) consistente en un ordenador, con una pistola simulada que había adquirido para ello, y de un Corán, además de un gesto con la mano amenazante. El texto de alguno de estos post fue del tenor siguiente: (24.07.2011)*" mata a un infiel y golpea a Europa y América, el paraíso se encuentra a las sombras de las espadas"… "Gente miembros de los foros de la fuerza y negación, gente del monoteísmo y la fe, despertados del sueño que se alegró y llevad armas encima, acechad a los turistas judíos y cristianos y los ayudantes del sistema tirano, extendeos en los países de occidente ocupante, no les dejéis disfrutar de la seguridad hasta que lo tengamos de verdad en nuestras tierras y se eleve la bandera del monoteísmo encima del Jerusalén ocupado. Atacad a los que rezan a la cruz, nuestros hombres de los foros como la mercancía de Dios es el paraíso, la mercancía de Dios es el paraíso, paraísos del Edén donde corren por debajo ríos, que vais a estar eternos en ellos... Los lobos corren detrás del que no tiene perros y se apartan del valiente... Juro por Dios que a nuestro honor no se le hará daño hasta que se derrame por sus lados la sangre... Gente de los foros yihadistas a por las armas del combate contra el enemigo en el corazón de Europa, América, y donde los encontréis, atacad sus tierras, envenenar sus aguas, explotad sus mercados y lugares de reunión, convertir sus noches en días y sus mañanas en fuego". "Dios mío, concédeme el martirio por tu causa, que tenga la valentía y la suficiencia, que mi cuerpo vuele en pedazos, por amor a ti, hasta el punto de no poder reunirlos para enterrarlos en la tumba. ¡Dios, amén!"* Algunos de estos posts con los que se habría conversación recibieron contestación de otros usuarios del foro, del tipo:... *"me has alegrado con tu foto de firma, aterrorízales héroe, que Dios te dé suerte terrorista".*

Tercero.- También Jaime administraba la página web llamada "*Shabaka Al Haqiqa Al Ikhbaria*" traducido "red de la verdad informativa", en la que para acceder a ella empleaba como nombre de usuario el mismo de la denominación de la página. Era una página no de participación, sino de descargas, y en la que como administrador colgaba imágenes, vídeos y noticias respecto de temas yihadistas, incluidos vídeos de acciones terroristas o de Al Qaeda, que pretendían ser

contrainformativas, y presentar la verdad desde el punto de vista radical yihadista, en contraposición a la verdad oficial difundida por los medios de comunicación social convencionales.

DECISIÓN

FALLO: QUE DEBEMOS DECLARAR Y DECLARAMOS NO HABER LUGAR AL RECURSO DE CASACIÓN interpuesto por la representación del acusado JAIME, contra sentencia dictada por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional, de fecha 12 de julio de 2003, en causa seguida contra el mismo por delito de pertenencia a organización terrorista y difusión del terrorismo en la que se le condena a 2 años de cárcel y 10 años de inhabilitación pública. Condenamos a dicho recurrente al pago de las costas procesales ocasionadas en su recurso. Comuníquese esta resolución a la mencionada Audiencia a los efectos legales oportunos, con devolución de la causa que en su día remitió.

Así por esta nuestra sentencia, que se publicará en la Colección Legislativa, lo pronunciamos, mandamos y firmamos.

D. CÁNDIDO CONDE PUMPIDO TOURÓN.

D. JULIÁN SÁNCHEZ MELGAR.

D. JOSÉ RAMÓN SORIANO SORIANO.

D. ALBERTO JORGE BARREIRO PERFECTO.

D. ANDRÉS IBÁÑEZ.

ARGUMENTO DE LA DECISIÓN

PROBLEMA JURÍDICO RESUELTO POR LA SENTENCIA

El recurrente en el primero de los dos motivos que alega, considera vulnerado el art. 24 CE en sus apartados 1º y 2º (tutela judicial efectiva y presunción de inocencia), aunque solo desarrolla y de forma muy escueta el último de los derechos fundamentales reseñados, protesta que canaliza a través del art.

5.4 LOPJ.

Con sede procesal en el art. 849.1º LECrim en relación al art. 20.1. a) y b) de la CE, por considerar que estaba ejercitando derechos fundamentales.

Se le condena en base al art. 579.1, par. 2º del CP (que castiga la distribución o difusión pública por cualquier medio de mensajes o consignas dirigidas a provocar, alentar o favorecer la perpetración de cualquiera de los delitos previstos en este capítulo de terrorismo).

RATIO DECIDENDI (rd) "la razón de la decisión"

PRIMERO

1. Considera que las escasas pruebas existentes son de naturaleza indiciaria, integradas fundamentalmente por el testimonio de los agentes policiales que intervinieron en el operativo y algún otro testigo, amén de lo depuesto por el propio encausado.

2. El Tribunal de instancia en su labor valorativa de la prueba rechaza el argumento fundamental del recurrente explicando las razones que darían al traste con tal pintoresca motivación de los hechos efectuada. En primer lugar no resulta en absoluto razonable la suplantación de un usuario, perfectamente detectable por el propietario, ya que cualquier intervención queda registrada en actividades del foro, además de la incompatibilidad con las propias medidas de seguridad normales en esta clase de foros cerrados que tratan de evitar ser observados por intrusos no pertenecientes a la comunidad.

SEGUNDO

1. Los preceptos constitucionales citados predican la libertad de expresión por cualquier medio, bien sea oral o escrito, con el único límite de los derechos de

los demás y el honor y la propia imagen.

2. A éste acusado solo se le condena en base al art. 579.1, par. 2º del CP que castiga "la distribución o difusión pública por cualquier medio de mensajes o consignas dirigidas a provocar, alentar o favorecer la perpetración de cualquiera de los delitos previstos en este capítulo (terrorismo), generando o incrementando el riesgo de su efectiva comisión".

3. Por otro lado y para restringir el ejercicio de los derechos fundamentales invocados por el recurrente, especialmente los de libertad ideológica y libertad de expresión, según la doctrina seguida por el TC. Así pues no se encontrarían bajo protección constitucional la realización de actos o actividades que, en el desarrollo de ciertas ideologías, vulneren otros derechos fundamentales, como ocurre en el presente caso.

TERCERO

La desestimación del recurso hace que las costas le sean impuestas al recurrente, de conformidad al art. 901 LECrim.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

- El Tribunal de instancia se basó en las siguientes pruebas:

a) La confesión en juicio del acusado.

b) El testimonio del instructor del atestado, guardia civil.

c) El contenido de los posts remitidos, como prueba documental.

- La finalidad crematística no resulta armonizable, con su actividad paralela y frenética en varios foros, incluso administraba uno de intercambio de vídeos y noticias. La motivación de la Sala es plenamente razonable y aceptable para esta Sala de casación.

- Libertad de expresión: denota inconstitucionalidad la realización de actos o actividades que, en el desarrollo de ciertas ideologías, vulneren otros derechos fundamentales, cosa que el tribunal observa claramente en el presente caso.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

V.6.- SENTENCIA 400/2016

V.6.1.- Análisis de la Sentencia

ROJ: STS 2031/2016 - ECLI:ES:TS:2016:2031
Nº Sentencia: 400/2016 **Tipo Órgano: Tribunal Supremo. Sala de lo Penal** **Municipio: Madrid -- Sección: 1** **Resumen: Delito de enaltecimiento del terrorismo.**

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	**Vicente Pons Gamón**
FECHA:	**07-01-2007**
PROYECTO:	**"Ciberterrorismo, legislación: aplicación y seguridad"**
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	**STS 2031/2016 - ECLI: ES:TS:2016:2031**
	Nº de Recurso: 115/2016 **Nº de Resolución: 400/2016**
FECHA y LOCALIDAD.	**MADRID – 11/05/2016**
PROCEDIMIENTO	**Penal procedimiento abreviado/sumario**
MAGISTRADO PONENTE:	**D. Manuel Marchena Gómez**
DEMÁS MAGISTRADOS	**D. José Ramón Soriano Soriano** **D. Francisco Monterde Ferrer** **D. Juan Ramón Berdugo Gómez de la Torre** **D. Perfecto Andrés Ibáñez**
VOTO PARTICULAR:	**No hay voto particular**

Ilustración 43: *STS 2031/2016 - ECLI: ES: TS: 2016:2031.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. MANUEL MARCHENA GÓMEZ, demás magistrados D. JOSÉ RAMÓN

SORIANO SORIANO, D. FRANCISCO MONTERDE FERRER, D. JUAN RAMÓN BERDUGO GÓMEZ DE LA TORRE y D. PERFECTO ANDRÉS IBÁÑEZ (ilustración 43), sin que se tenga constancia de voto particular.

En primer lugar el acusado se encontraba en España en situación administrativa irregular. Éste publicó en Internet, concretamente en "*YouTube*" un video elaborado por él, titulado: "Así me ha enseñado el Imán de los Imanes OUSSAMMA, que *Allah* lo acepte". Este tenía cinco partes, de diez minutos las 4 primeras y ocho minutos y cincuenta y seis segundos la última.Su narrativa era épica laudatoria, aparecían imágenes personales y de sus acciones, además de discursos de Santos llamando a hacer la Yihad, en claro homenaje a su figura, oratorias de otros líderes yihadistas como VICTORIO o CARLOS ALBERTO y también, imágenes de campos de entrenamiento de Al Qaeda. Igualmente constaban añadidos textos en árabe, presentando el video la "asociación de soldados de OUSSAMA" y cerrando el video: "*Allah*, haznos los mejores apoyos de los mejores Yihadistas".

El Juzgado Central de instrucción nº 4, incoó diligencias previas de procedimiento abreviado núm. 298/2008, contra el acusado. Una vez conclusas, lo remitió a la Sala de lo Penal de la Audiencia Nacional (Sección Segunda).Ésta dictó sentencia el 23 de noviembre de 2015 en causa seguida contra éste, y le condenócomo autor de un delito de enaltecimiento del terrorismo a la pena de 1 año y 6 meses de prisión, con la pena principal de inhabilitación absoluta durante 8 años.

El acusado presentó recurso al Tribunal Supremo que con fecha 23 de noviembre de 2015 falla en contra, no habiendo lugar a recurso de casación, confirmando la sentencia de la Audiencia Nacional y además condenándole al pago de las costas causadas por el recurso[314].

[314] Vid. STS, Sala de lo penal. nº 400 de 11 de mayo de 2016. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7676158&links=&optimize=20160519&publicinterface=true

V.6.2.- Aspectos de interés

NORMA DEMANDADA
APOLOGÍA DEL TERRORISMO
PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNALSUPREMO

Esta Sala, compuesta como se hace constar, ha visto el recurso de casación por infracción de ley, quebrantamiento de forma y vulneración de precepto constitucional interpuesto por la representación procesal de Esteban contra la sentencia dictada por la Sala de lo Penal de la Audiencia Nacional (Sección Segunda) de fecha 23 de noviembre de 2015 en causa seguida contra Esteban, por delito de enaltecimiento del terrorismo, los Excmos. Sres. componentes de la Sala Segunda del Tribunal Supremo que al margen se expresan se han constituido para Votación y Fallo bajo la Presidencia del primero de los citados. Ha intervenido el Ministerio Fiscal, el recurrente representado por la procuradora doña MARÍA CRISTINA MÉNDEZ ROCASOLANO. Siendo magistrado ponente el Excmo. Sr. D. MANUEL MARCHENA GÓMEZ.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

La sentencia núm. 32/2015, dictada por la Sección Segunda de la Sala Penal de la Audiencia Nacional en fecha 23 de noviembre de 2015, condenó al acusado ESTEBAN como autor de un delito de enaltecimiento del terrorismo a la pena de 1 año y 6 meses de prisión, con la pena principal de inhabilitación absoluta durante 8 años.

Se reacciona críticamente frente a lo que la defensa considera una vulneración del derecho a la inviolabilidad de las comunicaciones del art. 18.3 de la CE. También se censura la inaplicación de la atenuante de dilaciones indebidas.

DEMANDA

El Juzgado Central de instrucción nº 4, incoó diligencias previas de procedimiento abreviado nº 298/2008, contra ESTEBAN y, una vez concluso, lo

remitió a la Sala de lo Penal de la Audiencia Nacional (Sección Segunda) rollo de Sala de procedimiento abreviado núm. 3/2014 que, con fecha 23 de noviembre de 2015, dictó sentencia que contiene los siguientes:

HECHOS PROBADOS: PRIMERO.- El día 17 de mayo de 2011, el acusado ESTEBAN, con NIE 000, en situación administrativa irregular en España (f. 1.590), publicitó a través de Internet, mediante su subida a la aplicación "*YouTube*" un video elaborado en todo o en parte por él mismo, titulado: "Así me ha enseñado el Imán de los Imanes OUSSAMMA, que *Allah* lo acepte". El documental constaba de cinco partes, las cuatro primeras con una duración de diez minutos y la quinta de ocho minutos y cincuenta y seis segundos, compuesto en forma de narrativa épica laudatoria, apareciendo imágenes personales y de sus acciones, además de discursos de SANTOS llamando a hacer la *Yihad*, en claro homenaje a sufigura, oraciones de otros líderes yihadistas como VICTORIO o CARLOS ALBERTO e imágenes de campos de entrenamiento de Al Qaeda. Igualmente constaban añadidos textos en árabe, presentando el video la"asociación de soldados de OUSSAMA", y cerrando el video: *"Allah, haznos los mejores apoyos de los mejores Yihadistas"*. El video fue publicado en el canal *YouTube* de internet *molaomar1* con nombre de usuario DIRECCIÓN 001, utilizado por el acusado ESTEBAN para subir dicho video a la red. En el mismo canal de YouTube se habían publicado hasta el 28 de mayo de 2011, otros 28 videos de similares características y temática yihadista, de contenido radical y violento. En la entrada y registro judicialmente autorizada (auto de 1 de junio de 2011) en el domicilio utilizado por el acusado en el momento de su detención, sito en la Avda. DIRECCIÓN 000, bloque nº. 001, puerta nº. 002 de San Bartolomé de Tirajana (Las Palmas), se intervino una libreta notas, con páginas rayadas, que contenía textos en árabe y alfabeto español manuscritos por el acusado, entre los que, en su página 78, consistían en anotaciones de distintas claves de accesos a servidores wifi para acceso a Internet:nº. 007; nº. 008; nº. 009 y nº. 010.

DECISIÓN

FALLO. Que debemos declarar y declaramos NO HABER LUGAR al recurso de casación, interpuesto por la representación legal de Esteban contra la

sentencia de fecha 23 de noviembre de 2015, dictada por la Sección Segunda de la Sala Penal de la Audiencia Nacional, en la causa seguida por el delito de enaltecimiento del terrorismo y condenamos al recurrente al pago de las costas causadas. Comuníquese esta resolución a la Audiencia mencionada a los efectos legales procedentes, con devolución de la causa que en su día remitió, interesando acuse de recibo. Así por esta nuestra sentencia, que se publicará en la Colección Legislativa lo pronunciamos, mandamos y firmamos D. MANUEL MARCHENA GÓMEZ, D. JOSÉ RAMÓN SORIANO SORIANO, D. FRANCISCO MONTERDE FERRER, D. JUAN RAMÓN BERDUGO GÓMEZ DE LA TORRE, D. PERFECTO ANDRÉS IBÁÑEZ.

PUBLICACIÓN.- Leida y publicada ha sido la anterior sentencia por el Magistrado Ponente Excmo. Sr. D MANUEL MARCHENA GÓMEZ, estando celebrando audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Letrado/a de la Administración de Justicia, certifico.

ARGUMENTO DE LA DECISIÓN

PROBLEMA JURÍDICO RESUELTO POR LA SENTENCIA

El primero de los motivos se formula al amparo de los arts. 5.4 de la LOPJ y 852 la LECrim Denuncia infracción de precepto constitucional, "...en relación con el artículo 24 de la CE" (sic).

No existió vulneración alguna del derecho a la inviolabilidad del domicilio y, precisamente por ello, procede la desestimación del motivo por su falta de fundamento (art. 885.1 y 2 LECrim), art. 849.1 LECrim, infracción de ley, por indebida inaplicación de la atenuante de dilaciones indebidas, con el carácter de muy cualificada, prevista en el art. 21.6 del CP.

RATIO DECIDENDI (rd) "la razón de la decisión"

1.- La sentencia núm. 32/2015, dictada por la Sección Segunda de la Sala Penal de la Audiencia Nacional en fecha 23 de noviembre de 2015, condenó al acusadoEstebancomo autor de un delito de enaltecimiento del terrorismo.

2.- La lectura del desarrollo del motivo permite concluir que la vulneración de alcance constitucional que se denuncia sería la que afecta al derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE), por la irregularidad de la decisión jurisdiccional que acordó su interceptación. De ahí se derivaría -por la imposibilidad de utilización- una infracción del derecho a la presunción de inocencia, a raíz del efecto contaminante que esa prueba ilícita habría proyectado sobre el resto del material probatorio ponderado por la Audiencia.

3.-Está fuera de cualquier duda decíamos en la SSTS 245/2009, 6 de marzo y 598/2008, 3 de octubre, que las intervenciones telefónicas, cuando son empleadas como medio de investigación en un proceso penal, implican un altísimo grado de injerencia pública en el círculo de derechos fundamentales que nuestro sistema constitucional garantiza a cualquier ciudadano, en el presente caso las razones que avalan la constitucionalidad de la medida de intromisión del Estado en las comunicaciones.

4.- Se argumenta que el procedimiento se inició en el año 2008, se dictó con fecha 18 de octubre de 2010 auto de sobreseimiento provisional y con fecha 21 de diciembre de 2010 se dictó auto de reapertura del procedimiento. Durante todo ese tiempo -se arguye- el acusado no ha solicitado pruebas ni ha desplegado ninguna maniobra dilatoria.

En la STS 446/2015, 6 de julio, con cita de la STC 54/2014, 10 de abril,decíamos que para determinar si nos encontramos o no ante una vulneración del derecho a un proceso sin dilaciones indebidas (art. 24.2 CE) hemos de acudir a las pautas que nos ofrece nuestra doctrina, conforme a la cual este derecho está configurado como un concepto jurídico indeterminado que, por su imprecisión, exige examinar cada supuesto a la luz de aquellos criterios que permitan verificar si ha existido efectiva dilación y, en su caso, si ésta puede considerarse justificada, por cuanto “no toda infracción de los plazos procesales o toda excesiva duración temporal de las actuaciones judiciales supone una vulneración del derecho fundamental que estamos comentando”[315].

[315] Vid. STC 153/2005, de 6 de junio, FJ 2.

5.- El tercero de los motivos denuncia quebrantamiento de forma de los arts. 850 y 851 LECrim.

Sostiene la defensa que no existe diligencia por parte del secretario judicial del Juzgado Central de instrucción núm. 4 de Madrid de adveración de transcripciones de las conversaciones telefónicas. Su transcripción fue delegada en los agentes de la Policía Nacional. Con ello se habría vulnerado el derecho a un proceso con todas las garantías del art. 24 de la CE, así como el principio de seguridad jurídica del art. 9 del mismo texto constitucional. De entrada, el motivo se aparta de las exigencias técnicas impuestas por los arts. 873 y ss LECrim. Se recurre a una cita genérica de los arts. 850 y 851 LECrim, sin precisar en cuál de los apartados se basarían la impugnación. Y lo que se anuncia como un motivo por quebrantamiento de forma se torna en un motivo por vulneración de precepto constitucional. Con ello se incurre en la causa de inadmisión prevista en el art. 884.4 LECrim, que ahora actuaría como causa de desestimación. Sea como fuere, la jurisprudencia constitucional ha reiterado (por todas, SSTC 145/2014, 22 de septiembre; 126/2000, de 16 de mayo, FJ 9) que no constituyen una vulneración del derecho al secreto de las comunicaciones las irregularidades cometidas en el control judicial a *posteriori* del resultado de la intervención telefónica.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

La Sala se basa en sus decisiones en:

Por un lado la claridad de las pruebas aportadas en el juicio por los agentes intervinientes.

Las actuaciones policiales coordinadas con el orden jurisdiccional lo cual le da carácter de legalidad a las pruebas.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

V.7.- SENTENCIA 693/2016

V.7.1.- Análisis de la Sentencia

ROJ: STS 3691/2016 - ECLI:ES:TS:2016:3691
Nº Sentencia: 693/2016 **Tipo Órgano: Tribunal Supremo. Sala de lo Penal** **Municipio: Madrid -- Sección: 1** **Resumen: Pertenencia y dirección de organización terrorista y tenencia ilícita de armas. Intervenciones telefónicas. Identificación de las voces de los distintos interlocutores.**

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	**Vicente Pons Gamón**
FECHA:	**07-01-2007**
PROYECTO:	**"Ciberterrorismo, legislación: aplicación y seguridad"**
CONTEXTO	
IDENTIFICACIÓN	
NÚMERO:	**STS 3691/2016** **Nº de Recurso: 10896/2015** **Nº de Resolución: 693/2016**
FECHA y LOCALIDAD.	**MADRID – Madrid -- Sección: 1/27/07/2016**
PROCEDIMIENTO	**Penal - apelación procedimiento abreviado**
MAGISTRADO PONENTE:	**D. José Manuel Maza Martín**
DEMÁS MAGISTRADOS	**D. Julián Sánchez Melgar** **D. Antonio del Moral García** **Dña. Ana María Ferrer García** **D. Perfecto Andrés Ibáñez**
VOTO PARTICULAR:	**NO SE REALIZA VOTO PARTICULAR**

Ilustración 44: *STS 3691/2016.*

Sección primera del TS, procedimiento penal abreviado. El magistrado ponente es D. JOSÉ MANUEL MAZA MARTÍN, demás magistrados D. JULIÁN SÁNCHEZ MELGAR, D. ANTONIO DEL MORAL GARCÍA, D. ANA MARÍA FERRER GARCÍA y D. PERFECTO ANDRÉS IBÁÑEZ (ilustración 44), sin que se tenga constancia de voto particular.

A los acusados se les acusa por integración a organización terrorista perteneciente a Al Qaeda detectada en Ceuta y Marruecos en los primeros meses del 2012, cuyo propósito era crear la infraestructura necesaria para mandar combatientes al *Yihad* a Siria mediante su incorporación a alguna de las organizaciones terroristas que allí operaban y con el objetivo final de lograr el Califato mundial.Esta organización estaba formada por dos células, una con marroquíes y otra con españoles residentes en Ceuta. A partir de aquí comenzaron los desplazamientos de individuos desde Ceuta y Marruecos a Siria para el *Yihad*. Los Once acusados se integraron en la mencionada red yihadista de Ceuta, la cual actuaba en estrecha conexión con la célula de Fnideq en Marruecos.

Se tramitan once recursos, uno por acusado, contra la Sentencia dictada por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional, el 30 de septiembre de 2015, por delitos de dirección e integración en organización terrorista y tenencia ilícita de armas por la cual están condenados a:

Se condena a dos Acusados en concepto de dirigentes de organización terrorista a las penas de DOCE AÑOS DE PRISIÓN E INHABILITACIÓN ABSOLUTA POR VEINTE AÑOS, a cada uno de ellos.

Se condena a ocho Acusados en concepto de integrantes activos en organización terrorista a las penas de DIEZ AÑOS DE PRISIÓN E INHABILITACIÓN ABSOLUTA POR DIECIOCHO AÑOS, a cada uno de ellos.

Se condena a un Acusado en concepto del delito de tenencia ilícita de armas a las penas de UN AÑO Y SEIS MESES DE PRISIÓN e inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena.

El 27 de julio del 2016 el Tribunal Supremo, Sala primera, declara no haber lugar a la estimación de los Recursos de Casación interpuestos confirmando la sentencia de la Audiencia Nacional y condenándoles a las costas generadas por dicho recurso[316].

[316] Vid. STS, Sala de lo penal nº 693de 27 de julio de 2016. Recuperado de: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7746350&links=&optimize=20160729&publicinterface=true

V.7.2.- Aspectos de interés

NORMA DEMANDADA
Pertenencia y dirección de organización terrorista y tenencia ilícita de armas.
PROBLEMA JURÍDICO ENUNCIADO POR EL TRIB. SUPREMO

Sentencia dictada por la Audiencia Nacional, Sección 2ª que les condenó por:

1) Delito del art. 571.1º CP, en concepto de dirigentes de organización terrorista.

2) Delito del art. 571.2 CP, en concepto de integrantes activos de organización terrorista, y, por tenencia ilícita de armas.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

Esquema de recursos presentados por los acusados:

- RKA: Recurso de ABILIO EDUARDO (cinco motivos).
- RIA: Recurso de VIDAL NAZARIO (un único motivo).
- RAC: Recurso de INOCENCIO DONATO (cinco motivos).
- RMH: Recurso de IGNACIO TEODORO (dos motivos).
- RTM: Recurso de LAUREANO CRISTOBAL (tres motivos).
- RAA: Recurso de ALEXIS MAXIMINO (cuatro motivos).
- RYA: Recurso de JULIÁN TORCUATO (tres motivos).
- RAS: Recurso de EULOGIO BARTOLOMÉ (diez motivos).
- RAL: Recurso de GENARO DIONISIO (cinco motivos).
- RRA: Recurso de SANTOS ADOLFO (cinco motivos).
- RNA: Recurso de CONRADO LEÓN (cuatro motivos).

A) Falta de claridad en el relato de hechos probados (art. 851.1 LECrim).

B) Incongruencia omisiva (art. 851.3 LECrim), o “fallo corto”, en el motivo Cuarto del RAA, al no haberse ofrecido respuesta a alguna de las pretensiones del recurrente.

C) Inclusión en la narración de expresiones predeterminantes del Fallo ulterior (art. 851.1 LECrim), a las que se refieren el ya mencionado motivo Tercero del RYA y el Décimo del RAS.

D) A su vez, en otra serie de motivos se plantea, a través de los artículos 5.4 de la Ley Orgánica del Poder Judicial y 852 LECrim, en relación con el 18.3 y 24.1 y 2 de la CE, la supuesta vulneración de diferentes derechos fundamentales, que pasamos a examinar individualizadamente:

- Un proceso con garantías (arts. 18.3 y 24.2 CE), al que aluden los motivos Único del RIA, Primero del RAL y Segundos del RKA, del RAC, del RMH, del RNA, del RAL y del RNA.

- En cuanto a la infracción del derecho a la presunción de inocencia (art.24.2 CE) se refieren los motivos Único del RIA, Primeros del RKA, del RAC, del RMH, del RTM, del RAA, del RYA, del RAL y del RNA y Tercero del RAS.

E) Finalmente, los restantes motivos se refieren a diversas infracciones de Ley, por indebida aplicación de las normas de derecho sustantivo a los hechos declarados probados por el Tribunal *"a quo"* (art. 849.1º LECrim).

F) Los motivos Segundos del RAA y del RYA y Tercero del RTM versan, con cita del artículo 849.2º LECrim, sobre supuestos errores de hecho en los que habrían incurrido los Jueces *"a quibus"* a la hora de valorar la prueba documental obrante en las actuaciones.

- La correcta aplicación del artículo 571 CP vigente.

- La adecuada aplicación de los artículos 563 y 564 CP.

- La inaplicación del artículo 14 CP.

- A la indebida inaplicación de los artículos 16.3, 21. 7ª y 579 bis.

G) Dada la conclusión desestimatoria de los Recursos, procede, a tenor de lo dispuesto en el artículo 901 LECrim, la imposición a los recurrentes de las costas procesales causadas por cada uno de ellos.

DEMANDA

El Juzgado Central de Instrucción número 2 instruyó Sumario con el número 1/2014 y, una vez concluso, fue elevado a la Audiencia Nacional, Sección 2ª que, con fecha 30 de septiembre de 2015 dictó sentencia que contiene los siguientes HECHOS PROBADOS:

PRIMERO.- AL QAEDA es una organización terrorista que pretende la expulsión de los occidentales y el establecimiento de un Califato Islámico Mundial; imponiendo la aplicación estricta y radical de la Sharia o Ley Islámica; empleando para ello la violencia y siguiendo los postulados de la *Yihad* Global.

SEGUNDO.- En los primeros meses del año 2012 se detectó en Ceuta y Marruecos la creación de una organización yihadista cuyo propósito era mandar combatientes para hacer la *Yihad* a Siria mediante su incorporación a alguna de las organizaciones terroristas que allí operaban antes mencionadas y con el objetivo final de lograr el Califato mundial, sujeto a una aplicación estricta de la *shura*. En dicha organización se integraron dos células estrechamente vinculadas entre sí y que actuaban conjuntamente y con análogo *modus operandi,* una formada por marroquíes y otra por españoles residentes en Ceuta.

TERCERO.- En la creación de la infraestructura necesaria que permitiera el fluido y constante envío de combatientes a la zona y en el funcionamiento de la red, mediante la coordinación de los integrantes marroquíes y ceutíes y de los miembros de la Katiba a la que iban destinados tuvieron una función muy relevante el líder de la Katiba, ISIDORO TEODORO y 1 acusado, VIDAL NAZARIO, lo que dio lugar a la policialmente conocida como RED MAHDALI- AL LAL.

CUARTO.- A partir de la recepción de dicha autorización se iniciaron los desplazamientos de yihadistas desde Ceuta y Marruecos para incorporarse a la Yihad en Siria, los cuales se prolongaron durante todo el año 2012 y el 2013. El 7 de abril de 2.012, dos días después de ser recibida la mencionada orden, CIPRIANO NICOLÁS (Ganso), JACOBO LEÓNCIO (Chiquito), y BALBINO ABELARDO (Bucanero), se trasladaron en barco desde Ceuta hasta Algeciras y de allí a Málaga. El día 9, a las 14,10 horas CIPRIANO NICOLAS y JACOBO LEÓNCIO compraron billetes de avión

a Turquía; comprándolo BALBINO ABELARDO por la tarde, a las 19,22 horas. El citado CIPRIANO NICOLÁS (Ganso), viajó desde Málaga a Turquía el día 10 de abril y el 11 de abril de 2.012 lo hicieron JACOBO LEÓNCIO, (Chiquito) y BALBINO ABELARDO (Bucanero). Los tres emprendieron la marcha hacia Turquía tras sacar un pasaporte nuevo y cambiar su aspecto, cortándose el pelo y la barba, portando ropa occidental. De todas las gestiones relativas al viaje los mencionados voluntarios fueron dando cuenta vía telefónica al marroquí TOMAS IÑIGO, que correlativamente se comunicaba con VIDAL NAZARIO. Una vez en Turquía los tres desplazados, que habían hecho una reserva para el periodo comprendido entre el 12 y el 15 de abril en un hotel de Estambul, pasaron, sin embargo, a alojarse el día 13 en el hotel Mozaik de Antakya, provincia de Hatay, en el que permanecieron hasta el día 28 de abril en la habitación 205. El 29 de abril se trasladaron al Hotel Ceilán en Antakia (Hatay), donde se reunieron con VIDAL NAZARIO, que el día 26 de abril había vuelto a viajar desde Bruselas a Estambul; trasladándose a Hatay; hospedándose junto con ellos en el mencionado Hotel Ceylán entre el 29 de abril y el 2 de mayo; compartiendo con CIPRIANO NICOLÁS (Ganso) la habitaciónnº. 000, mientras que JACOBO LEÓNCIO (Chiquito) y BALBINO ABELARDO (Bucanero) compartían la nº. 001. Por su parte, varios marroquíes integrantes de la red habían viajado a Turquía desde Casablanca,TOMAS IÑIGO el día 20 de abril y REMIGIO, OSCAR, ROMEO y VICTORINO el 22 de abril; viajando después, el día 29 de abril, RUBÉN DONATO. De modo que el día 1 de mayo se reunieron en Hatay los cuatro ceutíes y los cuatro marroquíes citados. Ese mismo día 1 de mayo se alojaron en el mismo hotel Ceylán en el que se hospedaban los cuatro españoles y otros tres marroquíes, RUBÉN DONATO, SILVIO LUCIO y AMBROSIO DIMAS. Entre el día 2 y el 3 de mayo de 2.012 los españoles cruzaron la frontera a Siria. VIDAL NAZARIO, ejerciendo sus funciones de control de los miembros de la red, viajó nuevamente el 30 de mayo de 2.012 a Turquía, desplazándose desde Estambul a Hatay, volviendo el día 8 de junio a Estambul; regresando a Holanda el 9 de junio. Dicho viaje coincidió con el fallecimiento en atentado suicida del primero de los desplazados ceutíes. CIPRIANO NICOLÁS (Ganso), que había anunciado a través de un perfil en *Facebook* su determinación para la comisión de una acto de "martirio", utilizando la expresión "casado", que es uno de los términos usado en el *argot* yihadista para anunciar ese tipo de acciones, el 1 de junio de 2.012 se inmoló, conduciendo un camión cargado de explosivos contra el cuartel militar de Idlib en

Siria, ataque que fue seguido de otros con explosivos y bombas trampa contra el personal de los servicios de emergencias y refuerzo que llegó para socorrer a los heridos y repeler el ataque. JACOBO LEÓNCIO (Chiquito), y BALBINO ABELARDO (Bucanero), también fallecieron el 26 de junio de 2.012 en atentados suicidas en Siria. En concreto, BALBINO ABELARDO (Bucanero) murió explosionando un vehículo bomba contra un puesto de control de Al Bara, en el que fallecieron cien personas. Los meses siguientes continuaron los desplazamientos de integrantes de la célula, tanto desde España como desde Marruecos. El 29 de septiembre de 2.012, desde Madrid, viajaron los nacionales marroquíes con residencia en España CELSO URBANO y ELADIO ISMAEL, quienes fallecieron en Siria haciendo la Yihad. El 27 de diciembre de 2012 desde Madrid con destino final a Siria viajaron EZEQUIAS, ROGELIO y CECILIO PRIMITIVO, habiéndose incorporado ambos a la organización terrorista ESTADO ISLÁMICO DE IRAK Y LEVANTE (ISIL). El mencionado EZEQUIAS ROGELIO fue detenido en Marruecos, junto con otros, tras regresar de Siria, en marzo de 2.014. En el segundo semestre de 2012 también continuaron las salidas de marroquíes desde Casablanca. El día 14 de julio salieron cinco voluntarios, el 27 de julio de 2012 otros seis, el 30 de agosto uno y el 12 de octubre dos más. El 25 de marzo de 2013 viajó desde Casablanca el menor de edad VICTOR HIGINIO, *alias* Quico. El día 29 de marzo se desplazó desde Málaga GUILLERMO ERASMO, al que acompañó en el Ferry desde Ceuta a Algeciras IGNACIO TEODORO. El 29 de abril de 2013 viajó desde Málaga el acusado EULOGIO BARTOLOMÉ, pasando a Siria; llegando a la localidad de Atarib el 4 de mayo de 2013. El mismo fue detenido a la vuelta de Siria en enero de 2014. El 31 de mayo de 2013 viajaron desde Málaga a Turquía y desde allí a Siria ALFREDO GABINO (Gótico), VICENTE URBANO, FRANCISCO VIDAL (Chipirón) y JUAN ÓSCAR. Todos ellos se incorporaron al ISIL, aunque en facciones distintas. Al menos tres de los desplazados el 31 de mayo han fallecido en la comisión de acciones violentas; recibiendo sus familiares noticias telefónicas del fallecimiento. FRANCISCO VIDAL (Chipirón), conocido en la organización como ALFONSO PATRICIO, falleció el 11 de agosto cometiendo un atentado suicida con un cinturón de explosivos en ABU GHRAIB, Irak, acto que fue reivindicado por el ISIL; recibiendo su madre una llamada en la que le comunicaban su muerte, al día siguiente. VICENTE URBANO, al que llamaban Leovigildo Lázaro, murió en fecha próxima, sin que conste si fue en Siria o en Irak; siendo comunicada su muerte a la familia el 12 de agosto. ALFREDO

GABINO (Gótico), conocido en el grupo como NAZARIO NEMESIO, murió conduciendo un coche bomba probablemente en Irak; siendo comunicada su muerte a su esposa el 6 de septiembre. Respecto de JUAN ÓSCAR no consta su fallecimiento. El 15 de junio de 2013 se preparó una nueva expedición de cuatro integrantes de la célula ceutí para viajar a Siria. A tal fin, tres de los que iban a desplazarse, los acusados GENARO DIONISIO, SANTOS ADOLFO y CONRADO LEÓN, viajaron a Algeciras para comprar cuatro billetes a Turquía; efectuando diversas gestiones en varias agencias de viajes, de lo que iban informando telefónicamente al también acusado INOCENCIO DONATO, *alias* Tiburón, *alias* Tirantes, el cual les iba transmitiendo las órdenes de la forma en que deberían efectuar las búsquedas y de las medidas de seguridad que debían adoptar. Pese a haber buscado en múltiples agencias, no encontraron disponibilidad de vuelos, lo que comunicaron a INOCENCIO DONATO, el cual les transmitió finalmente la orden de que regresaran a Ceuta, instrucción que, a su vez, había dado el jefe de la célula ceutí, ABILIO EDUARDO, orden que fue acatada, regresando el mismo día los tres viajeros a Ceuta. Por su parte los días posteriores ABILIO EDUARDO, también realizó búsquedas de billetes para Turquía. La última remesa de voluntarios no llegó a desplazarse, por haberse producido el día 21 de junio de 2013 las detenciones de los acusados que se encontraban en Ceuta, con excepción de JULIÁN TORCUATO, que se dio a la fuga cuando iba a registrarse su domicilio; lográndose su detención el mes de septiembre del mismo año. VIDAL NAZARIO fue detenido en noviembre de 2013 en Bélgica y EULOGIO BARTOLOMÉ el 5 de enero de 2014, cuando regresaba de Turquía expulsado por las autoridades de dicho país.

QUINTO.- Los acusados en este procedimiento,ABILIO EDUARDO, INOCENCIO DONATO, IGNACIO TEODORO, LAUREANO CRISTÓBAL, ALEXIS MAXIMINO, VIDAL NAZARIO, JULIÁN TORCUATO, EULOGIO BARTOLOMÉ, GENARO DIONISIO, SANTOS ADOLFO y CONRADO LEÓN, se integraron en la mencionada red yihadista de Ceuta, la cual actuaba en estrecha conexión con la célula de Fnideq en Marruecos, conforme a los dictados de AL QAEDA y de las organizaciones adscritas a dicha organización terrorista citadas (JaN e ISIL), cuyo objetivo inmediato era el establecimiento del Estado Islámico en Siria y finalmente alcanzar el Califato Mundial,

SEXTO.- ABILIO EDUARDO, alias “Corsario”, era el director y principal responsable de la célula en Ceuta, Dirigía, coordinaba y controlaba las actividades

de los integrantes ceutíes y en parte de los marroquíes, atendidas la estrecha interrelación entre los dos grupos. La función de dirección y coordinación que ABILIO EDUARDO llevaba a cabo desde la ciudad autónoma abarcaba desde la captación, adoctrinamiento y preparación de los jóvenes yihadistas que habrían de desplazarse, pasando por la gestión de los viajes y control de los viajeros en las fechas inmediatamente anteriores a los desplazamientos, hasta el seguimiento de las actividades de los yihadistas desplazados, comunicación a las familias del estado de los incorporados a la Yihad, notificación, en su caso, de los fallecimientos y difusión de los actos de martirio. También recaudaba fondos para su envío a los desplazados en Siria y, en caso necesario, para asistencia a las viudas. Así, ABILIO EDUARDO, desempeñaba un papel esencial en la captación y radicalización de jóvenes para participar en la Yihad en Siria, para lo cual disponía en su ordenador, intervenido en el registro practicado el día 21 de junio de 2013 en su domicilio, sito en la BARRIADA 000, DIRECCIÓN 000 nº. 002 de Ceuta, de material de propaganda, consistente en audios que ensalzaban la Yihad en Siria. Entre las mencionadas grabaciones se encontraba la publicada por "la brigada de los muyahidines en Siria", en la que se incitaba a la Yihad en dicho país por parte de un grupo de muyahidines armados; varios discursos de diversos líderes salafistas, entre otros, el pronunciado por FERMÍN TEODOSIO, emir de JABHAT AL MURABITIN FI ZUGHUR BILAD AL SHAM, organización terrorista que opera en Siria. También fueron hallados vídeos, en los que se observaba a los yihadistas despidiéndose y realizando con posterioridad atentados suicidas.

SÉPTIMO.- INOCENCIO DONATO, *alias* "Tiburón" o "Tirantes" actuaba en la célula terrorista como lugarteniente de ABILIO EDUARDO; transmitiendo a sus integrantes las órdenes impartidas por el mismo; ejerciendo funciones de control sobre los yihadistas que estaban próximos a ser enviados a Siria; participando de forma destacada en la organización y supervisión de los viajes y posteriormente en el seguimiento de las actuaciones de los desplazados; dando información a las familias sobre su situación. Por otro lado, intervenía, junto con los restantes acusados, en actividades desplegadas tanto en Ceuta como en Marruecos para la radicalización religiosa y preparación física previas a las salidas hacia Siria. Para el ejercicio de las funciones de captación y adoctrinamiento poseía vídeos sobre JABHAT AL NUSRAH y ANSAR AL SAHARIA, documentación que proclamaba la

Yihad global, múltiples cánticos y oraciones ensalzando la Yihad y pidiendo venganza mediante la misma y alabanzas a las acciones de las milicias yihadistas. Dicha documentación audiovisual fue intervenida en el registro de su domicilio, sito en BARRIADA 000 DIRECCIÓN 001 nº.004 de Ceuta. Igualmente se intervino en el registro de su domicilio un Documento Nacional de Identidad a nombre de SANTOS ADOLFO que ejercía también funciones de coordinación con los integrantes de la célula marroquí, para lo cual cruzaba con frecuencia la frontera, acompañado de otros miembros de la red que posteriormente se desplazaron a Siria. También ejercía labores de supervisión sobre los jóvenes que iban a incorporarse a la Yihad en Siria, con los que se reunía.

OCTAVO.- IGNACIO TEODORO *alias* "Millonario" era uno de los integrantes de célula ceutí y ejecutaba los actos que la misma le encomendaba, al servicio de la tarea común de envío de voluntarios para hacer la yihad en Siria e integrarse en las organizaciones terroristas dependientes de AL QAEDA que allí operaban. Al igual que los otros acusados, participó asiduamente en reuniones y sesiones en las que se preparaban para incorporarse a la Yihad, tanto mediante la radicalización ideológica como mediante el adiestramiento para el combate. Con tal finalidad poseía libros en formato digital en los que se alababa la lucha contra los enemigos de su religión, entre los que se encontraban "los Frutos de la Yihad dedicado a cada predicador y yihadista con intención de marcharse". Igualmente disponía de un CD con archivos sobre la Yihad, entre los que se encontraba un vídeo titulado "Así se preparan los leones del Frente Al Nusra", campamento militar "los leones de la nueva Gloria", en el que se muestra el entrenamiento armado de los yihadistas en dicho campamento y el vídeo "Al Nusra" y el ESTADO ISLÁMICO, lanzar flechas contra aquel que dijo que Siria no necesita hombres; descubrir a los fracasados. Así como dos libros de adoctrinamiento del Islam salafista de titulo "AL WALAE WA AL- BARAE RM EN EL ISLAM" (Lealtad a Dios y hostilidad para los enemigos de Dios y combatirlos y "Lealtad a Allah y hostilidad para los enemigos de Allah y combatirlos desde la doctrina salafista") de MOHAMED BES SAID BEN SALEM AL QATHANI, sobre JABHAT AL NUSRAH. Igualmente, disponía de dos manuales para la fabricación de explosivos caseros.

NOVENO.- LAUREANO CRISTÓBAL *alias* "Chillón", era miembro de la organización y participaba junto con los demás, en las actividades de captación y

preparación para la yihad en Siria, antes mencionadas, algunas de las cuales se celebraban en Ceuta y otras en Marruecos. Efectuaba funciones de seguimiento de la preparación de los viajes y desarrollaba una transcendental función de comunicación con los integrantes de la red en Siria. Para la referida labor de captación y adoctrinamiento disponía de diversos archivos y documentos relacionados con el ESTADO ISLÁMICO DE IRAK, discursos, imágenes de contenido yihadista que fueron intervenidos en un dispositivo Blakberry 9300 que fue hallado en el registro de su domicilio.

DÉCIMO.- ALEXIS MAXIMINO, *alias* Corretejaos o Capazorras, se constituyó en el referente ideológico de los integrantes de la célula. Realizaba una importante labor de captación y adoctrinamiento de personas para combatir en Siria. Encabezó las actuaciones de radicalización religiosa realizadas por la red. Desplegó, junto con otros acusados, funciones de acompañamiento y control de los voluntarios hasta el momento del viaje y con posterioridad. Una vez producida la salida de los voluntarios, efectuaba un seguimiento telefónico de la situación de los desplazados; manteniendo para ello diversas comunicaciones con Turquía y Siria. Con la mencionada finalidad de captación y adoctrinamiento de jóvenes candidatos para hacer la yihad en Siria, a los que los integrantes de la red se referían como “los chicos”, ALEXIS MAXIMINO poseía abundante documentación yihadista, que fue intervenida en el registro de su domicilio. Entre otros, más de cien audios ensalzando a los muyahidines y a los mártires, el discurso “la Yihad es una lección del pueblo”, una arenga del fundador de AL QAEDA en Irak,Leopoldo Humberto, y un audio editado por KATIBAB Al Nusra, órgano de comunicación de JABHAT Al Nusra, en el que se sintetiza el planteamiento ideológico y la acción de JABHAT Al Nusra, se recoge un llamamiento a la Yihad en Irak y se declara la autoridad de AL QAEDA sobre el ISIL. Participó en reuniones de radicalización religiosa protagonizadas por importantes jeques salafistas que desempeñaron un papel esencial en la dinamización del envío de yihadistas a Siria, cuyas enseñanzas transmitía. En concreto, participó en una reunión celebrada en Castillejos el 16 de noviembre de 2012, en la que los líderes religiosos PASCUAL OLEGARIO, COSME EVERARDO, HIGINIO PATRICIO y ISMAEL NEMESIO formularon arengas en apoyo de la Yihad.

DECIMOPRIMERO.- VIDAL NAZARIO, *alias* "Santo", llevó a cabo una actuación esencial para el establecimiento en Siria de la infraestructura a la que posteriormente iban a incorporarse los miembros de la célula ceutí y muchos de los de la marroquí; desplegando también un papel decisivo en la efectividad de las incorporaciones de yihadistas a dicho país. Supervisó y controló personalmente las salidas y fundamentalmente las llegadas de los voluntarios enviados por ambas células para hacer la yihad en Siria y controló la efectiva realización de los actos de martirio planeados por la organización y posteriormente reivindicados por JABHAT *Al Nusra*o por el ISIL. Igualmente contribuyó a la coordinación entre los integrantes marroquíes y ceutíes, con la finalidad de que se incorporaranmaterialmente a la yihad en Siria y ejecutaran acciones violentas al servicio de los fines perseguidos por dichas organizaciones. A tales fines se desplazó a Turquía, Ceuta y/o Marruecos en fechas especialmente significativas, por coincidir, bien con el establecimiento de la infraestructura necesaria y llegada del que sería futuro líder de la Katiba, bien con desplazamientos de voluntarios tanto ceutíes como marroquíes que, una vez incorporados, se inmolaron o ejecutaron atentados con múltiples víctimas, bien con momentos en que se iban a ejecutar los atentados o en que se iban a comunicar los fallecimientos de los "mártires".

VIDAL NAZARIO tenía una vinculación antigua con JACOBO LEÓNCIO (Chiquito) y CIPRIANO NICOLÁS (Ganso), dos de los primeros ceutíes desplazados a Siria, al menos desde que coincidió con ellos en el año 2009, época en la que los tres estuvieron con ESTANISLAO LORENZO *alias* Pelos, condenado en Marruecos por terrorismo islámico y liberado en 2008, el cual fue detenido en Marruecos nuevamente en mayo de 2009; librando las autoridades marroquíes orden de detención de CIPRIANO NICOLÁS (Ganso) y JACOBO LEÓNCIO (Chiquito), momento a partir del cual estos dejaron de entrar en Marruecos para evitar ser capturados. VIDAL NAZARIO regresó a Bruselas, sin volver a detectarse su presencia en España hasta el año 2012. Con anterioridad al primero de los desplazamientos de voluntarios ceutíes a Siria VIDAL NAZARIO había vuelto a contactar en Ceuta con CIPRIANO NICOLÁS (Ganso) y JACOBO LEÓNCIO (Chiquito); tomando parte en reuniones y en algunos de los partidos de fútbol organizados por éstos, los cuales eran aprovechados para captar y entrenar jóvenes que pudieran incorporarse a la

causa yihadista. En los periodos en que VIDAL NAZARIO estaba en Ceuta y Marruecos participaba en las reuniones, actividades y encuentros de los miembros de la red utilizadas para la captación, adoctrinamiento de yihadistas y consolidación de los vínculos existentes entre ellos. VIDAL NAZARIO fue el primero de los integrantes de la red que llegó a Turquía, el 1 de abril de 2012, con la finalidad de preparar la logística necesaria para la llegada de los yihadistas marroquíes y ceutíes a Siria. Allí coincidió con el futuro líder de la Katiba TARIK Ibn Ziad, ISIDORO TEODORO (el cual llegó a Turquía el día 4 de abril de 2012). Su estancia también coincidió con la llegada de otro de los principales miembros de la célula marroquí, BRAULIO JAVIER.

En el domicilio en Bélgica de VIDAL NAZARIO se intervino su ordenador, en el que fueron recuperados datos de búsquedas en Internet relacionadas con la guerra en Siria, consultas sobre CIPRIANO NICOLÁS (Ganso), vídeos de acciones terroristas cometidas por *Al Nusra*, audios y vídeos sobre combates en Siria, vídeos relacionados con JABHAT *Al Nusra*, materiales destinados a la propagación de las ideas de incorporación a la Yihad. Parte de esas búsquedas se efectuaron inmediatamente antes del primer desplazamiento a Turquía de VIDAL NAZARIO.

DECIMOSEGUNDO.- JULIAN TORCUATO, *alias* Zurdo, era miembro de la célula de Ceuta dedicada al envío de yihadistas a Siria y tomaba parte asiduamente en las actividades de la misma. A tal fin mantenía contactos continuos con ABILIO EDUARDO, ALEXIS MAXIMINO, IGNACIO TEODORO, SANTOS ADOLFO, LAUREANO CRISTÓBAL, GENARO DIONISIOy con ALFREDO GABINO. JULIÁN TORCUATO era uno de los miembros de la organización que estaba preparado para desplazarse a Siria; no pudiendo hacerlo cuando lo hicieron sus compañeros FRANCISCO VIDAL, (Chipirón), ALFREDO GABINO, (Gótico), VICENTE URBANO y JUAN ÓSCARque marcharon el 31 de mayo de 2013; estando dispuesto a partir para incorporarse a hacer la yihad en dicho país en cuanto fuera posible. Participaba en las actividades de radicalización religiosa desplegadas por los integrantes de la célula. Así, entre finales de febrero y principios de marzo de 2013, acudió, junto con ABILIO EDUARDO, ALEXIS MAXIMINO, SANTOS ADOLFO, un hermano de JACOBO LEÓNCIO (Chiquito) y FRANCISCO VIDAL (Chipirón) a la mezquita Bard; advirtiendo a los asistentes de que si el Imán no cambiaba el tipo de lectura coránica, cerrarían

las puertas de la misma, al no atenerse a lo que se leía en la mezquita *Atawha*; siendo el principal instigador de lo ocurrido ALEXIS MAXIMINO; produciéndose durante las discusiones entre el grupo mencionado y los asistentes a la mezquita una agresión por parte de ABILIO EDUARDO, al Imán, cuando éste les invitó a que abandonaran el recinto; habiendo cerrado CORSARIO las puertas de la mezquita, prohibiendo que se abrieran hasta que se cumpliera lo establecido por ellos. JULIÁN TORCUATO tomaba parte, junto con los restantes acusados, en las actividades realizadas en la playa y en los partidos de fútbol en Ceuta y Marruecos que eran aprovechadas para adoctrinar y entrenar a los futuros desplazados, a los que los integrantes de la red se referían como "los chicos". También asistió a reuniones en el domicilio de ALEXIS MAXIMINO y a diversos encuentros preparatorios llevados a cabo por los miembros de la red en fechas próximas a los desplazamientos a Siria. Entre otras, a las reuniones en la playa mantenidas entre el 11 y el 15 de junio de 2013, a las que asistieron también ALEXIS MAXIMINO, IGNACIO TEODORO, GENARO DIONISIO, SANTOS ADOLFO y LAUREANO CRISTOBAL. Con el propósito de desplazarse a Siria, junto con la expedición de yihadistas que viajaron el día 31 de mayo de 2013, JULIÁN TORCUATO inició los preparativos habitualmente realizados por todos los miembros de la red que iban a partir; concretamente, la obtención de nuevo pasaporte, en el que no constaran los sellos de las salidas anteriores y cambió de imagen, cortándose el pelo y afeitándose la barba. Finalmente no llegó a marcharse; habiendo acudido a su casa los demás integrantes de la expedición para despedirse de él. Los días inmediatamente anteriores a que se produjera dicho desplazamiento de los yihadistas que salieron el 31 de mayo y que intentaron despedirse de JULIÁN TORCUATO, éste estuvo visionando en el teléfono numerosos vídeos y audios, entre otros, vídeos del ISIL, que incluían doctrina de carácter general, transmitida por destacados dirigentes de AL QAEDA

Este acusado, que estaba dispuesto a marcharse a hacer la Yihad en cuanto fuera posible, se dio a la fuga cuando iba a ser detenido el 21 de junio de 2013, fecha en que se produjo la detención de la mayoría de los acusados pertenecientes a la célula. No obstante se logró su detención tres meses después, sin que pudieran ser intervenidos materiales yihadistas, ni otros dispositivos o elementos de interés.

DECIMOTERCERO.- EULOGIO BARTOLOMÉ, *alias* Botines, era uno de los integrantes de la célula ceutí que participaba junto con los demás en reuniones de adoctrinamiento y entrenamiento previas a la marcha a Siria para hacer la yihad; manteniendo contactos con los restantes integrantes de la red, fundamentalmente con ABILIO EDUARDO, y con otro de los yihadistas que posteriormente se desplazó también a Siria, ELISEO JUSTINIANO (Pulpo). EULOGIO BARTOLOMÉ, tras "occidentalizar su apariencia", recortándose el pelo y la barba y utilizar ropa occidental, abandonó la ciudad autónoma de Ceuta con dirección a Marruecos el día 29 de abril de 2013. El día 1 de mayo tomó un vuelo en el aeropuerto de Casablanca con destino a Turquía, entró en dicho país el día 2 de mayo y desde allí se desplazó a Siria; incorporándose a las filas del ISIL, participando en acciones de dicha organización tanto en Siria como en Irak. Tras llegar a Siria fue a la localidad de Atarib, a un campamento de entrenamiento y formación de la organización ISIL, utilizando el nombre de CAMILO MANUEL, campo de entrenamiento en el que encontró a otros miembros de la red, que se desplazaron el 31 de mayo de 2.013, ALFREDO GABINO, VICENTE URBANO, FRANCISCO VIDAL (Chipirón) y JUAN OSCAR y el menor VICTOR HIGINIO. A finales de junio de 2013 entró en Irak y participó en la misión de liberar prisioneros de la cárcel de ABU GHRAIB, situada en Bagdad. Ese ataque fue reivindicado por el ISIL el día 23 de julio de 2013, también marchó a zonas no determinadas para combatir. Durante su estancia en Siria, por otro lado, usaba el mismo número de teléfono sirio que era utilizado por otros integrantes de la red, entre ellos, por FRANCISCO VIDAL (Chipirón). Dicho teléfono se encontraba entre los contactos telefónicos de LAUREANO CRISTÓBAL y de ALEXIS MAXIMINO y que fue recuperado en el momento de su detención. Tras haber estado ocho meses en las filas del ISIL, este acusado regresó desde Siria a Turquía y voló desde Antaquia a Estambul; donde adquirió un billete con destino a Amsterdam, el cual no llegó a utilizar, dado que fue expulsado por las Autoridades de Turquía a España al tener caducado el visado. El mismo fue detenido el 5 de enero de 2.014 en el puesto fronterizo del aeropuerto de Málaga; interviniéndosele los billetes de avión a Turquía y de Turquía a Amsterdam y un móvil, en el que el mismo tenía guardado un archivo de audio con un cántico de alabanza del ISIL, denominado "El francotirador de nuestro Estado".

DECIMOCUARTO.- Genaro Dionisio, Virutas, era uno de los integrantes de la célula yihadista de Ceuta. Fue uno de los miembros de la misma que intentó desplazarse a Siria el 15 de junio de 2013. Genaro Dionisiose incorporó a una ciber-comunidad, creada a principios de 2012, a través de los contactos de CIPRIANO NICOLÁS (Ganso) en *Facebook*, a la que pertenecían un gran número de yihadistas, tanto de Ceuta como de Marruecos, entre otros, TOMÁS IÑIGO, ROMEO VICTORINO y REMIGIO ÓSCAR. GENARO DIONISIOse incorporó a dicha red, mediante la cual algunos seguían contactando una vez que se habían marchado a Siria. Este acusado, a través de una cuenta en *Facebook*, con el alias de DIRECCIÓN 003, ensalzaba la Yihad en Siria. Participaba en las actuaciones comunes de los miembros de la célula para la captación y adoctrinamiento de yihadistas y para su envío a Siria.

Con dicha finalidad disponía en su domicilio de videos y audios, en los que se ensalzaba la yihad y se justificaban las acciones de martirio; llamando a la incorporación de estos métodos en Siria. Entre otros, un vídeo con el título “Los Mejores Mártires”, en el que se señalaba que “martirio” es sacrificarse para defender el Islam; distinguiendo las operaciones de martirio, que se consideran un valor de valentía del musulmán, de los actos de suicidio. Igualmente, disponía de un vídeo en el que aparecían niños vestidos con uniforme miliar y portando armas, en el que cantaban, incitando a la yihad y al martirio. Esos materiales fueron intervenidos en diversos dispositivos hallados en el registro de su domicilio. Mantenía también contactos con destacados jefes salafistas marroquíes que dinamizaban el envío de yihadistas a Siria, en concreto, con PASCUAL OLEGARIO. Junto con LAUREANO CRISTÓBAL y JUAN ÓSCAR, GENARO DIONISIO mantenía frecuentes contactos con otros integrantes tanto de Marruecos como de Ceuta.

DECIMOQUINTO.SANTOS ADOLFO, *alias* Cachas, era otro de los integrantes de la célula que participaba en las actividades comunes dirigidas a la captación, adoctrinamiento y envío de yihadistas a Siria.

Para el cumplimiento de los fines de la organización, SANTOS ADOLFO estaba en contacto frecuente con los otros integrantes de la red, fundamentalmente con ABILIO EDUARDO, su tío, del que recibía instrucciones directamente o a través de INOCENCIO DONATO; contactando también frecuentemente con LAUREANO

CRISTÓBAL, ALEXIS MAXIMINO, IGNACIO TEODORO, JULIÁN TORCUATO, GENARO DIONISIO y CONRADO LEÓN. Realizaba una intensa actividad de adoctrinamiento. A tal fin, disponía en su domicilio de material destinado a la radicalización religiosa. Entre otros, se le ocuparon numerosos discos de audio, en algunos de los cuales Imanes predicadores del Corán transmiten mensajes anticristianos y antisemitas. Transmitía o recibía de otros yihadistas comunicaciones anunciando cursos y sermones de jefes salafistas. Entre finales de febrero y principios de marzo de 2013 formó parte de un grupo de alborotadores musulmanes pertenecientes a la mezquita Atawba que se personaron en varias ocasiones en la mezquita Bard de la misma ciudad. Este acusado acudió a dicha Mezquita junto con ABILIO EDUARDO, ALEXIS MAXIMINO, JULIÁN TORCUATO, un hermano de JACOBO LEÓNCIO (Chiquito) y FRANCISCO VIDAL (Chipirón). Los mismos advirtieron a los asistentes a la mezquita de que en caso de que el Imán no cambiara el tipo de lectura coránica, cerrarían las puertas, al no atenerse ésta a lo que se leía en la mezquita Atawha; siendo el principal instigador de lo ocurrido ALEXIS MAXIMINO. Durante las discusiones entre el grupo mencionado y los asistentes ABILIO EDUARDO llegó a agredir al Imán, cuando éste les invitó a que abandonaran el recinto y acto seguido CORSARIO cerró las puertas de la misma; prohibiendo que se abrieran hasta que se cumpliera lo establecido por ellos.

En el registro practicado en el domicilio de SANTOS ADOLFO, sito en la BARRIADA 000 DIRECCIÓN 001 nº. 021 de Ceuta, se intervino una escopeta de cañones recortados con el número de serie 022, un revolver marca AMADEO ROSSI con número de serie 023, calibre 38 especial, un cartucho del calibre 12 y un cartucho de calibre 9, una bolsa con munición y una pistola simulada marca Walter modelo CP99. La escopeta y el revólver estaban en buen estado de funcionamiento y eran aptos para el disparo. El acusado guardaba un recorte de prensa sobre la desaparición de Ceuta de EULOGIO BARTOLOME. En dicho domicilio se intervinieron dos pasaportes españoles, uno a nombre de AGAPITO NARCISO, nº. 024, pasaporte del que consta una denuncia por su sustracción y otro a nombre de FERNANDO PLÁCIDO, nº. 025.

DECIMOSEXTO.- CONRADO LEÓN, *alias* Topo, era otro de los integrantes de la célula que participaba en las actividades comunes de adoctrinamiento y entrenamiento para el envío de yihadistas a Siria y era uno de los que debería

haber viajado a dicho país el 15 de junio de 2013. A tal fin, CONRADO LEÓN tenía en su domicilio, sito en laCALLE 000 nº. 026 de Ceuta, numerosos audios ensalzando la *Yihad* y discursos de los líderes de Al-Qaeda, en los que se llamaba a la guerra; recordando la obligación de los musulmanes de odiar a los judíos y a los cristianos, que el enemigo es occidente y el pueblo americano y que hay que castigarlo; así como una grabación en la que se pide la destrucción de los EE.UU. y la de todos los infieles y que maten al Presidente de EE.UU. Intervino en actividades de la célula tendentes a la radicalización religiosa y ensalzamiento de los atentados cometidos en Siria.

Así, en agosto de 2012, CONRADO LEÓN, con otros miembros de la organización, tomó parte en un encierro de diez días que tuvo lugar en la mezquita Atawba de Ceuta en honor de CIPRIANO NICOLÁS (Ganso), JACOBO LEÓNCIO (Chiquito) y BALBINO ABELARDO (Bucanero), primeros desplazados a Siria en abril de 2012 y que murieron en atentados suicidas reivindicados por JABHAT AL NUSRAH. En ese encierro estuvieron también, ABILIO EDUARDO, IGNACIO TEODORO, SANTOS ADOLFO, JULIÁN TORCUATOY ALFREDO GABINO (Gótico) y CIPRIANO NICOLÁS, hermano de CORSARIO.

Participaba junto con los restantes integrantes de la red en las actividades de adoctrinamiento y entrenamiento. Para el desarrollo de los fines mencionados mantenía una estrecha relación con otros integrantes de la red.

Se desplazó a Algeciras el 15 de junio para comprar los billetes para ir a Turquía y desde allí a Siria. Durante el desplazamiento habló con Inocencio DONATO y le comunicó (como ya lo había hecho SANTOS ADOLFO) la inexistencia de pasajes, preguntando si se quedaban allí o si regresaban a Ceuta, recibiendo, al igual que SANTOS ADOLFO, la orden de volver. En el momento de su detención se dirigió a los agentes, profiriendo gritos reiterados de “ALA AKBAR” (Alá es grande), grito de guerra de los radicales islamistas. Durante el registro de su domicilio lanzó a los funcionarios policiales actuantes la amenaza: “Suerte que no hay guerra, habrá, asquerosos hijos de puta, necesitan bombas”.

DECISIÓN

FALLO

Que debemos declarar y declaramos no haber lugar a la estimación de los Recursos de Casación interpuestos por las Representaciones de ABILIO EDUARDO, VIDAL NAZARIO, INOCENCIO DONATO, IGNACIO TEODORO, LAUREANO CRISTÓBAL, ALEXIS MAXIMINO, JULIÁN TORCUATO, EULOGIO BARTOLOMÉ, GENARO DIONISIO, SANTOS ADOLFO y CONRADO LEÓN contra la Sentencia dictada por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional, el 30 de Septiembre de 2015, por delitos de dirección e integración en organización terrorista y tenencia ilícita de armas. Se imponen a los recurrentes las costas procesales ocasionadas por sus respectivos Recursos.

La sentencia de instancia dictó el siguiente pronunciamiento:

FALLAMOS: Que debemos condenar y condenamos a ABILIO EDUARDO y VIDAL NAZARIO, en concepto de autores de un delito del art. 571.1 CP vigente en la fecha de comisión de los hechos, en concepto de dirigentes de organización terrorista, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a las penas de DOCE AÑOS DE PRISIÓN E INHABILITACIÓN ABSOLUTA POR VEINTE AÑOS, a cada uno de ellos.

Igualmente, debemos condenar y condenamos aINOCENCIO DONATO, IGNACIO TEODORO, LAUREANO CRISTÓBAL, ALEXIS MAXIMINO, JULIÁN TORCUATO, EULOGIO BARTOLOMÉ, GENARO DIONISIO, SANTOS ADOLFOyCONRADO LEÓN, en concepto de integrantes activos en organización terrorista, delart. 571.2 CP vigente en la fecha de comisión de los hechos, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a las penas de DIEZ AÑOS DE PRISIÓN E INHABILITACIÓN ABSOLUTA POR DIECIOCHO AÑOS.

Igualmente, debemos condenar y condenamos, a SANTOS ADOLFO, en concepto de autor de un delito de tenencia ilícita de armas de fuego delart. 564.1 y 2, en relación con elart. 564.2 3 del CP vigente en la fecha de comisión, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a las penas de UN AÑO Y SEIS MESES DE PRISIÓN e inhabilitación especial para el

derecho de sufragio pasivo durante el tiempo de la condena.

RATIO DECIDENDI (rd) "la razón de la decisión"

La decisión de ratificar la sentencia por parte del Tribunal Supremo se basa fundamentalmente por la claridad de hechos y pruebas y la confirmación de la actuación Judicial de forma correcta en el Juicio.

ARGUMENTOS NO ESENCIALES
INTERVENCIONES

Vicios *"in iudicando"* inexistentes:

- Falta de claridad de los hechos probados, predeterminación del Fallo ni incongruencia omisiva. Intervenciones telefónicas. Identificación de los interlocutores.
- Tutela judicial efectiva.
- Presunción de inocencia. Inexistencia de "*error facti*".
- Inexistencia de error de prohibición, desistimiento activo.
- Colaboración con las autoridades ni atenuante analógica de condena del terrorismo.

VOTO PARTICULAR (SV) (principales argumentos)
NO HAY VOTO PARTICULAR

CAPÍTULO VI

PERCEPCIÓN SOCIAL. ENCUESTAS

VI.1.- PERCEPCIÓN SOCIAL

La sociedad es consciente del grave peligro que supone la delincuencia en el ciberespacio y más concretamente los posibles actos terroristas que se pueden cometer a través de éste. La magnitud que pueden alcanzar estos ataques y el reto que supone para los estados poder establecer un ciberespacio seguro donde se respeten los derechos humanos es tan grande que desde un principio los estados y últimamente la sociedad en su conjunto están volcados en la búsqueda de la seguridad en el ciberespacio.

La Ciberdelicuencia y el Ciberterrorismo abarcan desde los miles de delitos cometidos por suplantación de identidad con robo económico, hasta el posible ataque de una infraestructura crítica como pueda ser una central nuclear o una presa.

Hasta hace poco gran parte de la sociedad no era consciente de la existencia de diferentes modalidades de ataques ciberterroristas, de sus posibles consecuencias y de las dificultades para controlarlas por parte de las fuerzas de seguridad del estado.

Recientemente, desde que se han producido repetidos y continuados ataques de tipo terrorista en diferentes países, la sociedad ha empezado a relacionar acciones terroristas con posibles resultados y consecuencias, dándose

cuenta de las magnitudes destructivas alcanzables y pidiendo prioridad a los estados para su control.

El problema puede ser tan grave y preocupante que podría desestabilizar un estado, dejando éste en situación de caos.

La sociedad es consciente de ello y ésto queda reflejado en diferentes encuestas realizadas en países de la UE donde queda plasmado como problema prioritario el terrorismo y dentro de éste el cibernético para el conjunto de la ciudadanía europea.

Por ejemplo, en la ilustración 45, observamos del Barómetro del Real Instituto Elcano (BRIE) en enero de 2016, las respuestas a la pregunta ¿cuál le parece que son las principales amenazas del exterior que pueden afectar a España?

Ilustración 45: *Percepción social del terrorismo Yihadista en España*[317].

[317] REAL INSTITUTO ELCANO. (Enero 2016). Percepción social del terrorismo yihadista en España. Fernando Reinares. Comentario Elcano 2/2016-25/1/2016,*Estudios Internacionales y Estratégicos*, Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/comentario-reinares-percepcion-social-terrorismo-yihadista-espana

"Las Fuerzas de Seguridad han registrado en los dos primeros meses de 2018 más incidentes de ciberseguridad en infraestructuras críticas que en todo 2014 (125 frente a las 63 de hace cuatro años) y la mayoría han sido intentos de escaneo de red o ataques con programas maliciosos para dañar equipos informáticos"*[318]*.

Este artículo publicado hace unos días por el periódico *El Mundo*, uno de los periódicos de más tirada en España y leído por millones de usuarios, habla muy claro de cuál es la situación actual de los ciberataques en nuestro país; del incremento desproporcionado de éstos desde el 2014.

Además del alcance de la prensa en los ciudadanos, según nuestros datos gran cantidad de usuarios de internet ha sufrido algún tipo de incidente en la red, bien sea un simple ataque de virus, algún intento de suplantación etc… por lo que entendemos que la población tiene muy clara cuál es la situación actual en la red y a lo que todos los usuarios nos exponemos cada día al usarla.

Por otro lado, la Encuesta Mundial sobre el Estado de la Seguridad de la Información de 2017, refleja que, desde 2012, las empresas han duplicado el presupuesto medio que dedican a ciberseguridad en el mundo, pasando de 2,8 a 5,1 millones de dólares, por lo que casi se ha duplicado. En España, la inversión de las compañías en seguridad de la información ha ha pasado de 3,1 a 3,9 millones de dólares de media, por lo que ha seguido una evolución parecida. Cada vez más las compañías utilizan la nube para almacenar sus documentos tecnológicos y de seguridad[319]. En este sentido, según PwC la ciberseguridad es la principal preocupación de los ejecutivos que asegura que el 89% en este sector, está preocupado ante la posibilidad de ser víctima de un ataque cibernético[320].

[318] AGENCIA EFE. (31 marzo 2018). España registra en 2 meses mas incidentes de ciberseguridad que en todo el 2014. *El Mundo.* Madrid. Recuperado de: http://www.elmundo.es/espana/2018/03/31/5abf4d9e268e3ebc098b4586.html

[319] Vid. PwC. Recuperado de: https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html

[320] EL ECONOMISTA. (17 de abrli de 2018). la ciberseguridad es la principal preocupación de los ejecutivos. Recuperado de: http://www.eleconomista.es/tecnologia/noticias/9078001/04/18/La-ciberseguridad-la-principal-preocupacion-de-los-ejecutivos-bancarios-segun-PwC.html

También en la encuesta de conocimiento sobre ciberseguridad que *InnoTec* (grupo *Entelgy*)[321] realizó en diciembre de 2017, se desprende, entre otras cosas, que: el 57,1% de las empresas ha realizado un hacking ético o auditoría de seguridad; un 81,3% dispone de un sistema de monitorización de seguridad que le permite detectar y gestionar incidentes; el 34,1% de los encuestados indican que no han implementado en su organización un plan de respuestas a incidentes[322].

Igualmente en la encuesta realizada por la Unión Internacional de Telecomunicaciones (UIT) en 2016 (ilustración 46), demuestran la inquietud y preocupación generalizada por la ciberseguridad, así: el 48% estiman poco segura las redes de comunicación, especialmente internet; el 80% señaló que la privacidad es un aspecto importante especialmente de la navegación por internet, pero sólo el 56% consideró que se respeta; la inquietud mencionada con mayor frecuencia, es el robo de información personal. En cuanto a la detección y divulgación de contenido ilegal, sitios electrónicos inapropiados y/o utilización indebida de internet, sólo el 40% de las respuestas estaban al corriente de los procedimientos de notificación en su país; sobre la importancia de la seguridad y medidas de seguridad "en línea", casi la mitad de los encuestados consideran que la estabilidad y la seguridad de la red son "muy importantes" y otra tercera parte la consideran "importante"[323]

[321] Principal socio del CCN-CERT Centro Criptológico Nacional y patrocinador VIP de las XI Jornadas STIC CCN-CERT

[322] Vid. Entelgy Blog Corporativo. Recuperado de: https://blog.entelgy.com/encuesta-ciberseguridad/

[323] Vid. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, UIT. (2018). Encuesta sobre ciberseguridad año 2016. Recuperado de: https://www.itu.int/itunews/manager/display.asp?lang=es&year=2006&issue=05&ipage=ITU-survey&ext=html

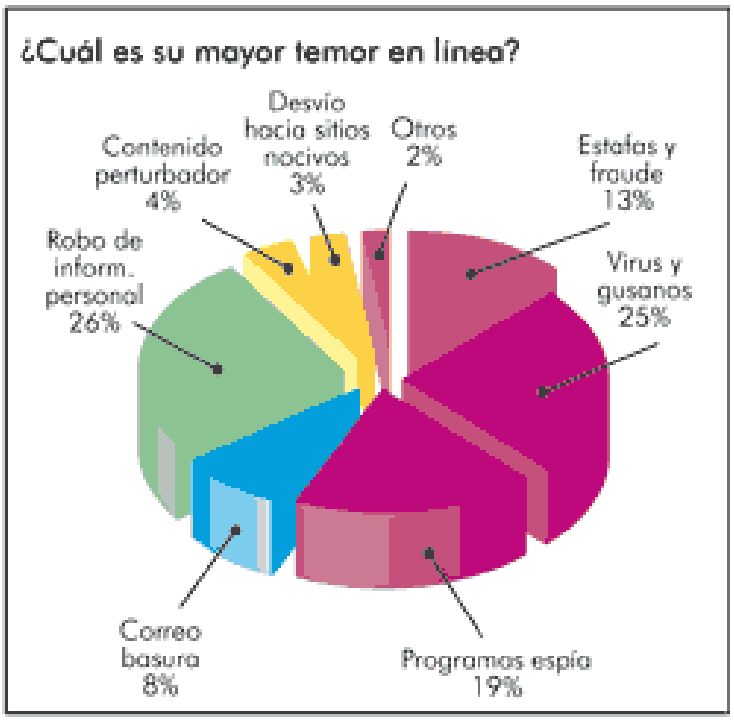


Ilustración 46: *Encuesta de la UIT sobre ciberseguridad en línea, 2016*[324]*.*

Por último, en el informe del "Special Eurobarometer 464a" sobre actitud de los europeos hacia la seguridad cibernética de junio de 2017, se optiene unos resultados que es preciso destacar[325]:

- La mayoría de los encuestados (56%) considera que la ciberseguridad es un desafío "muy importante" para la seguridad interna de la UE[326]:
    - Más de ocho de cada diez (87%) ven el cibercrimen como un desafío importante, un aumento significativo en el 80% registrado en marzo de 2015. El aumento es aún más significativo cuando se analiza la proporción de encuestados que ven el cibercrimen como un desafío muy importante: 56% comparado con 42% en 2015.
    - Existen diferencias significativas entre los países en la proporción

[324] Ibídem.
[325] EUROPEAN UNION. (junio de 2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. EU Open Data Portal. Recuperado de: https://data.europa.eu/euodp/data/dataset/S2171_87_4_464A_ENG
[326] Ibídem., p. 8.

de encuestados que piensan que el delito cibernético es un desafío muy importante, que varía del 76% en Chipre y del 75% en los Países Bajos a solo el 39% en Suecia y el 26% en Estonia.

  - Menos de la mitad (49%) de los encuestados están de acuerdo o mayormente de acuerdo en que las Fuerzas y Cuerpos de seguridad están haciendo lo suficiente para combatir el delito cibernético, y la proporción de encuestados que aceptan totalmente es baja en todos los Estados miembros. Además, una proporción significativa (14%) no sabe si se está haciendo lo suficiente para combatir el delito cibernético.

- El uso diario de Internet continúa aumentando en toda la UE, independientemente de los medios de acceso (casa, dispositivo móvil, en el lugar de trabajo o en la escuela / universidad).

  - Siete de cada diez encuestados (70%) usan Internet a diario y otro 9% lo hace a menudo o algunas veces.
  - Sin embargo, todavía hay diferencias significativas a nivel de país, y los países de Europa occidental y septentrional generalmente tienen más probabilidades de utilizar Internet a diario.
  - También existen importantes disparidades sociodemográficas en el acceso a Internet: los jóvenes (96%), los bien educados (87%), los económicamente seguros (73%) y los urbanos (75%) tienen más probabilidades de utilizar Internet. diariamente que las personas mayores (40%), aquellos con bajos niveles de educación (30%), los económicamente inseguros (58%) y aquellos que viven en aldeas rurales (64%).

- En la mayoría de los Estados miembros, menos de la mitad de los encuestados consideran que están bien informados sobre el delito cibernético. Existe una tendencia general que en los países donde los encuestados tienen más probabilidades de sentirse informados sobre los riesgos de los delitos informáticos, los encuestados también perciben el delito cibernético como una amenaza muy importante.

- Una mayoría creciente de encuestados está preocupada por experimentar o ser víctimas de los delitos cibernéticos, pero pocos realmente los han experimentado.

    - La mayoría de los encuestados están preocupados por ser víctimas de diversas formas de ciberdelincuencia, con la mayor proporción de encuestados que expresan preocupación por descubrir software malicioso en sus dispositivos (69%), robo de identidad (69%) y fraude bancario en línea y tarjetas bancarias (66%).
    - Menos de la mitad de los encuestados han sido víctimas de las diversas formas de cibercrimen. Las dos situaciones más comunes experimentadas por los encuestados son descubrir software malicioso en su dispositivo (42%) y recibir un correo electrónico o una llamada telefónica solicitando fraudulentamente el acceso a su computadora, inicios de sesión o datos personales (38%).
    - La mayoría de los encuestados informaría a la policía si fueron víctimas de cualquiera de los tipos de delitos informáticos considerados en este estudio, a excepción del descubrimiento de software malicioso en sus dispositivos; para este tipo de cibercrimen, informarán a su proveedor de servicios de Internet.

VI.2.- REALIZACIÓN DE ENCUESTAS

Para completar la investigación hemos realizado un trabajo de campo que consiste en la realización de tres tipos de encuestas a tres diferentes grupos de opinión:

- Grupo 1. Muestra de Fuerzas y Cuerpos de Seguridad del Estado.
- Grupo 2. Muestra de Magistrados y Jueces españoles.
- Grupo 3. Muestra de Letrados colegiados en España.

Estos grupos ejercen diferentes funciones dentro de las actuaciones contra el terrorismo, pero guardan relación y están interrelacionados entre sí. De hecho sus actuaciones son determinantes para combatir el fenómeno terrorismo-ciberterrorismo.

El primer grupo “FCSE” ha realizado una encuesta mucho más completa y amplia ya que nos interesa su opinión de temas generales sobre el terrorismo, temas de la parte legal y sobre todo su opinión de la parte operativa, un total de 17 preguntas.

El segundo grupo de opinión “Magistrados y Jueces” tiene una encuesta mucho más corta compuesta de unas pocas preguntas de aspectos generales sobre el terrorismo y sobre todo centrada principalmente en su opinión sobre la parte legal, una encuesta de ocho preguntas.

El tercer grupo de opinión “Letrados españoles” tiene una encuesta igual que la de los Jueces, mucho más corta compuesta de unas pocas preguntas de aspectos generales sobre el terrorismo y sobre todo centrada principalmente en su opinión sobre la parte legal, una encuesta de ocho preguntas.

Nos gustaría saber la opinión de los agentes de las fuerzas de seguridad, que en su mayoría reciben formación tanto general como legal centrada en terrorismo-ciberterrorismo.

También buscamos comparar las opiniones de dos grupos de profesionales del derecho, los jueces y los letrados, analizando la opinión de cada grupo desde su punto de vista.

Las preguntas realizadas son preguntas que se dividen en tres grupos:

- Aspectos generales: datos y definiciones técnicas sobre el terrorismo y ciberterrorismo.
- Aspectos prácticos: aspectos de la operativa diaria al respecto del terrorismo y ciberterrorismo.
- Aspectos legales: relacionados con temas de legalidad y las nuevas modificaciones producidas en las leyes españolas específicas sobre el

terrorismo y ciberterrorismo.

En el próximo punto analizaremos los resultados que utilizaremos principalmente de forma determinante para analizar nuestras hipótesis, datos que hemos obtenido de manera aleatoria y que de forma satisfactoria nos aclaran las diferentes visiones del problema general estudiado, el terrorismo y ciberterrorismo y sobre todo determina claramente que no es un problema estable, sino que cambia contínuamente. De esta forma las armas legales y operativas para combatirlos así como las opiniones de los grupos analizados, evolucionan y cambian contínuamente según el tiempo y la situación social del momento. Es decir si realizáramos las mismas encuestas a los mismos grupos y personas en un par de años, con total seguridad los resultados serían diferentes.

En este punto vamos a realizar una encuesta y análisis de forma individual de cada grupo de opinión.

VI.2.1.- Resultados encuesta FCSE

Encuesta CIBERTERRORISMO

(Abril 2017)

Respuestas recibidas: 125. - Preguntas: 18.

1. Perfil encuestado
Oficial Guardia Civil (Alférez, Teniente, Capitán, Comandante, Teniente Coronel, Coronel).
Oficial Fuerzas de Seguridad de otros países (Chile, Argelia, otros).
Profesor Universidad UC3M.

2. Indique unidad destino o destinos en los que haya estado (puede marcar varias)	
Seguridad Ciudadana/Puestos/Compañía:	37 (29,60 %)
Policía Judicial:	14 (11,20 %)

Información:	6 (4,80 %)
Unidad Central Operativa:	1 (0,80 %)
Especialidades de la GC:	20 (16,00 %)
Estado Mayor/Secretaría Técnica:	2 (1,60 %)
Órganos Centrales:	15 (12,00 %)
Dirección:	2 (1,60 %)
Asesoramiento:	2 (1,60 %)
Enseñanza, alumnos:	61 (48,80 %)
Otras:	42 (33,60 %)

3. (Aspectos generales) A su opinión, ¿qué tanto por ciento tiene el peso de la tecnología en la lucha antiterrorista?	
90%:	38 (30,40 %)
70%:	73 (58,40 %)
50%:	13 (10,40 %)
30%:	1 (0,80 %)

4. (Aspectos generales) ¿Un Hacker puede luchar contra el terrorismo en internet?	
Cualquier ciudadano puede colaborar con las Fuerzas y Cuerpos de Seguridad:	65 (52,00 %)
Tendría que ser un Hacker con un perfil concreto, equilibrado y fiable:	49 (39,20 %)
Solo si es "contratado" por las Fuerzas y Cuerpos de Seguridad:	9 (7,20 %)
NO:	2 (1,60 %)

5. (Aspectos generales) ¿Qué papel pueden jugar las redes sociales (Facebook, Twitter, Youtube, Telegram…)?	
Su colaboración tendría que ser obligatoria para que aporten los datos de almacenamiento de todos los usuarios:	41 (32,80 %)
Su colaboración tendría que ser inmediata en caso de usuarios sospechosos:	68 (54,40 %)
Solo tienen que colaborar cuando sea se hayan producido casos graves:	15 (12,00 %)
No tienen que colaborar:	1 (0,80 %)

6. (Aspectos generales) ¿Ha accedido en alguna ocasión en alguna "Deep Web"de contenido yihadista o similar?	
No:	86 (68,80 %)
Solamente las conozco:	31 (24,80 %)
Si he accedido como curiosidad:	6 (4,80 %)
Si he accedido para investigar:	2 (1,60 %)

7. (Aspectos generales) ¿Qué es lo que más destacaría de una web yihadista?	
Difusión de acciones:	29 (23,20 %)
Comunicación entre terroristas:	10 (8,00 %)
Financiación terrorista:	7 (5,60 %)
Captación terrorista:	79 (63,20 %)

8. (Aspectos legales) La LO 2/2015 introduce una amplia modificación del capítulo VII del título XXII del libro II del CP ("De las organizaciones y grupos terroristas y de los delitos de terrorismo"), ¿considera suficientes estas modificaciones?	
No las conozco:	54 (43,20 %)
Supone una disminución de los derechos del ciudadano:	0
Si, son suficientes en este momento a nivel operativo de fuerzas de seguridad:	5 (4,00 %)
Si, son suficientes a nivel judicial:	10 (8,00 %)
Si, son suficientes operativa y judicialmente:	11 (8,80 %)
No, deberían estudiarse aumentar otras medidas:	45 (36,00 %)

9. (Aspectos legales) ¿Cree que los terroristas conocen las leyes sobre antiterrorismo y sus actualizaciones?	
No:	43 (34,40 %)
Solamente las conocen:	20 (16,00 %)
Si, las conocen y buscan sus posibles vacíos a la hora de actuar:	62 (49,60 %)

10. (Aspectos legales) En su opinión, las fuerzas de seguridad ¿encuentran obstáculos legales a la hora de actuar contra una acción terrorista?	
Si, los necesarios, es fácil actuar:	18 (14,40 %)
Si, muchos obstáculos, es difícil de actuar:	88 (70,40 %)
No, se actúa con total profesionalidad, lo primero es la seguridad:	19 (15,20 %)

11. (Aspectos legales) ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para actuar con máxima eficacia y rapidez?	
Necesitan más especialización:	36 (28,80 %)
Siempre es bueno mejorar la formación:	88 (70,40 %)
No necesitan nada:	1 (0,80 %)

12. (Aspectos legales) ¿Conoce los desarrollos normativos antiterroristas de la Unión Europea y de Naciones Unidas?	
Si, los de la Unión Europea:	15 (12,00 %)
Si, los de Naciones Unidas:	1 (0,80 %)
Si, ambos:	25 (20,00 %)
No:	84 (67,20 %)

13. (Aspectos operativos) ¿considera adecuado el actual mecanismo de denuncia ciudadana en caso de un posible acto terrorista?	
Si:	78 (62,40 %)
No:	47 (37,60 %)

14. (Aspectos operativos) De entre las siguientes, ¿qué amenaza considera más peligrosa?	
Sabotaje informático:	36 (28,80 %)
Espionaje informático:	8 (6,40 %)
Difusión propaganda terrorista:	13 (10,40 %)
Ataque al sistema financiero:	19 (15,20 %)
Ataque al control de tráfico aéreo:	40 (32,00 %)
Ataque a sistemas de circulación terrestre:	9 (7,20 %)

15. (Aspectos operativos) ¿Conoce cómo trabajan los Equipos de Respuesta a Incidentes de Seguridad Informática CSIRT de su organización?	
Si:	17 (13,60 %)
No:	108 (86,40 %)

16. (Aspectos operativos) ¿Qué opina sobre uno de los puntos de la Línea de acción 1 de la Estrategia de Ciberseguridad Nacional de 2013 "Garantizar la coordinación, la cooperación y el intercambio de información entre diversos actores"?	
Hace falta definir los mecanismos de alto nivel para favorecer el intercambio de información:	41 (32,80 %)
Hay que favorecer el intercambio de información entre el sector público y privado:	73 (58,40 %)
Es inevitable que no se produzca un intercambio de información:	11 (8,80 %)

17. (Aspectos operativos) Considera que España está preparada para la ciberdefensa.	
Solo para acciones de defensa pasiva:	59 (47,20 %)
Si, para acciones reactivas que aseguren el uso de ciberespacio:	34 (27,20 %)
Si, para cualquier reacción incluso ciberataque contra el enemigo:	32 (25,60 %)

18. Añada cualquier comentario sobre aspectos generales, legales y operativos.
Hay que controlar sus finanzas y sus recursos porque creo que la mejor respuesta es evitar la publicidad y la propaganda que realizan dado que incita a la violencia y al terrorismo.
Es imprescindible fomentar la concienciación de todos los usuarios en el campo de la ciberseguridad y la formación de aquellos servicios especializados en la lucha contra el ciberterrorismo, ciberactivismo, ciberespionaje, etc.
En el campo de la investigación criminal, debe garantizarse la formación especializada del investigador a la vez de dotarle de máquinas e instrumentos jurídicos que posibilite su intervención eficaz.
En general pienso que la actuación de las FFCCS es muy buena en materia de terrorismo, sin embargo, es necesario estar siempre alerta y la comunicación entre ellos es un aspecto crucial y uno de los cuales debería mejorar.
España va un poco atrasada informáticamente, pero impulsa bastantes iniciativas para informatizar sistemas y procesos. Esto puede provocar indefensión al principio de la implantación de estos sistemas, ya que no está extendida una correcta mentalidad sobre seguridad informática en el usuario final.
Durante las asignaturas, he tenido la oportunidad de conocer las Estrategias y Legislación de España y Europa, así como algunas vivencias o experiencias de Tenientes, Capitanes y Comandantes, que han participado en algunas conferencias. Sé que tal vez la práctica sea distinta a la teoría, pero percibo una gran concienciación por parte de los integrantes de la Guardia Civil, para hacer frente a estas amenazas.
En comparación con otros países, como puede ser el caso de EE.UU., Rusia, China, Reino Unido, Francia, Alemania, etc. creo que España no está preparada para la lucha contra el ciberterrorismo.
La Ciberseguridad nos afecta a todos y el ciberterrorismo es una amenaza real.

En general considero que una parte importante de la seguridad en el uso de las tecnologías de información reside en la formación y la concienciación del personal que las manipula. Invertir en este campo generaría grandes beneficios en materia de seguridad dado que actualmente, el elemento más vulnerable de los sistemas son los propios usuarios, y se hace muy necesaria la formación del personal en su ámbito de actuación a todos los niveles, haciendo extensivo un plan de trabajo a todas las escalas del Cuerpo, que proporcionara los elementos de apoyo necesarios para prevenir en la medida de lo posible, la perpetuación de ataques informáticos que pusieran en riesgo la integridad, la disponibilidad o la confidencialidad de los datos que se manejan. En materia de Ciberseguridad ante elementos terroristas creo que el principal foco de riesgo está en las redes sociales, dado que a día de hoy su uso está generalizado casi en la totalidad de la población, y resulta especialmente sencillo adoctrinar sobre todo a la población más joven desde la distancia, sin necesidad de tener una infraestructura física de soporte, ni la influencia presencial que puede proporcionar un grupo, lo que aumenta el riesgo considerablemente.
Debe incrementarse el gasto en ciberseguridad.
En mi opinión, hasta el momento no hay incidentes que se puedan considerar como “ciberterrorismo”. De hecho, aunque la mayoría de los grupos terroristas aprovecharon la revolución de la información para establecer su presencia en la web con el fin de recaudar fondos, reclutar y difundir propaganda no censurada. Hasta ahora el ciberespacio ha sido utilizado por terroristas debido a su efecto multiplicador en términos de recopilación de información y definición objetivos, no como un arma ofensiva. En opinión de algunos expertos, parece poco probable que se convierta en un arma; a pesar de que se pueda ignorar por completo la amenaza debido a la rápidez de los avances tecnológicos y los cambios en la capacidad de los Grupos terroristas, los políticos y los expertos deberían aumentar e incidir en la necesidad de la cobertura mediática con respecto a este tema.
Con el ejemplo del reciente atentado en Londres; donde se ha pedido a Whatsapp su colaboración; hasta que no vuelva a ocurrir en España otro atentado de dimensiones parecidas al 11-M; no se actuará en nada al respecto para conseguir obligar a las aplicaciones de mensajería móvil a proporcionar datos sobre las conversaciones, si quieren operar en territorio nacional.
Pienso que en cuanto a ciberseguridad, estamos muy por debajo de lo deseable, creo que no hay una costumbre en España de darle mucha importancia a ésto como pasa en otros países o al menos así lo creo (Rusia, EE.UU.). Creo que tenemos grandes expertos, pero carencia de medios y de una conciencia social que hagan que los gobiernos financien y potencien fuertemente los medios de seguridad en el ciberespacio. Digamos que, la única formación que he recibido en este ámbito ha sido en la enseñanza superior (universidad).

VI.2.2.- Resultados encuesta Jueces

Encuesta CIBERTERRORISMO

(Abril 2017)

Respuestas Recibidas: 10. - Preguntas: 9

1. Perfil encuestados
Magistrado / Juez
Valencia
Derecho Penal, Civil y Mercantil

2. Aspectos generales. ¿En su opinión, cuáles son los delitos terroristas más frecuentes?	
Captación de adeptos en sus filas:	0
Enaltecimiento del terrorismo:	10 (100,00 %)
Humillación a las víctimas:	0
Intento o realización de acciones o atentados terroristas:	0

3. Aspectos generales. ¿Qué papel pueden jugar las redes sociales (Facebook, Twitter, Yotube, Telegram...) y sus datos en la lucha antiterrorista?	
Su colaboración tendría que ser obligatoria para que aporten los datos de almacenamiento de todos los usuarios:	0
Su colaboración tendría que ser inmediata en caso de usuarios sospechosos:	0
Solo tienen que colaborar cuando se hayan producido casos graves:	5 (50,00 %)
No tienen que colaborar:	5 (50,00 %)

4. Aspectos generales. ¿Considera adecuadas y suficientes las opciones de denuncia y aviso en caso de un posible delito terrorista, a disposición del ciudadano?	
Si:	10 (100,00 %)
No:	0

5. Aspectos legales. ¿Sabe cuáles son las principales diferencias de la Ley Orgánica 10/1995 del 23 de noviembre CP con las nuevas modificaciones del 2015 en materia antiterrorista?	
Si:	4 (40,00 %)
No:	0
No la he estudiado con detenimiento:	6 (60,00 %)

6. Aspectos legales. La LO 2/2015 introduce una amplia modificación del capítulo VII del Título XXII del libro II del CP (de las organizaciones y grupos terroristas y de los delitos de terrorismo), ¿considera suficientes y realistas estas modificaciones?	
No las conozco:	0
Supone una disminución de los derechos del ciudadano:	0
Si, son suficientes en este momento a nivel operativo de fuerzas de seguridad:	0
Si, son suficientes a nivel judicial:	9 (90,00 %)
Si, son suficientes operativa y judicialmente:	1 (10,00 %)
No, se debería estudiar aumentar más medidas:	0

7. Aspectos legales. ¿Cree que los terroristas conocen las leyes sobre terrorismo y sus actualizaciones?	
No:	2 (20,00 %)
Solamente las conocen los dirigentes:	7 (70,00 %)
Si las conocen y buscan sus posibles vacíos a la hora de actuar:	1 (10,00 %)

8. Aspectos legales. ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?	
Necesitan más especialización:	0
Siempre es bueno mejorar la formación:	5 (50,00 %)
No necesitan nada:	5 (50,00 %)

9. Aspectos legales. ¿Hay necesidad de reglamentar una Ley europea de seguridad antiterrorista cibernética?	
Si:	7 (70,00 %)
No:	0
No he estudiado el tema:	3 (30,00 %)

VI.2.3.- Resultados encuesta Letrados

Encuesta CIBERTERRORISMO

(Abril 2017)

Respuestas Recibidas: 20. - Preguntas: 9

1. Perfil encuestados
Abogado
Valencia, Barcelona, Madrid Posgrado o Doctor
Licenciado / Posgrado o Doctor
Derecho Penal, Civil, Administrativo y Mercantil

2. Aspectos generales. ¿En su opinión, cuáles son los delitos terroristas más frecuentes?	
Captación de adeptos en sus filas:	11 (55,00 %)
Enaltecimiento del terrorismo:	9 (45,00 %)
Humillación a las víctimas:	0
Intento o realización de acciones o atentados terroristas:	0

3. Aspectos generales. ¿Qué papel pueden jugar las redes sociales (Facebook, Twitter, Youtube, Telegram...) y sus datos en la lucha antiterrorista?	
Su colaboración tendría que ser obligatoria para que aporten los datos de almacenamiento de todos los usuarios:	4 (20,00 %)
Su colaboración tendría que ser inmediata en caso de usuarios sospechosos:	10 (50,00 %)
Solo tienen que colaborar cuando se hayan producido casos graves:	6 (30,00 %)
No tienen que colaborar:	0

4. Aspectos generales. ¿Considera adecuadas y suficientes las opciones de denuncia y aviso en caso de un posible delito terrorista, a disposición del ciudadano?	
Si:	14 (70,00 %)
No:	6 (30,00 %)

5. Aspectos legales. ¿Sabe cuáles son las principales diferencias de la Ley Orgánica 10/1995 del 23 de noviembre CP con las nuevas modificaciones del 2015 en materia antiterrorista?	
Si:	6 (30,00 %)
No:	8 (40,00 %)
No la he estudiado con detenimiento:	6 (30,00 %)

6. Aspectos legales. La LO 2/2015 introduce una amplia modificación del capítulo VII del Título XXII del libro II del CP (de las organizaciones y grupos terroristas y de los delitos de terrorismo), ¿considera suficientes y realistas estas modificaciones?	
No las conozco:	6 (30,00 %)
Supone una disminución de los derechos del ciudadano.	2 (10,00 %)
Si, son suficientes en este momento a nivel operativo de fuerzas de seguridad:	1 (5,00 %)
Si, son suficientes a nivel judicial:	3 (15,00 %)
Si, son suficientes operativa y judicialmente:	5 (25,00 %)
No, se debería estudiar aumentar más medidas:	3 (15,00 %)

7. Aspectos legales. ¿Cree que los terroristas conocen las leyes sobre terrorismo y sus actualizaciones?	
No:	2 (10,00 %)
Solamente las conocen los dirigentes:	10 (50,00 %)
Si las conocen y buscan sus posibles vacíos a la hora de actuar:	8 (40,00 %)

8. Aspectos legales. ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?	
Necesitan más especialización:	6 (30,00 %)
Siempre es bueno mejorar la formación:	12 (60,00 %)
No necesitan nada:	2 (10,00 %)

9. Aspectos legales. ¿Hay necesidad de reglamentar una Ley europea de seguridad antiterrorista cibernética?	
Si:	14 (70,00 %)
No.:	0
No he estudiado el tema:	6 (30,00 %)

CONCLUSIONES

PRIMERA: Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente. La era de la información multiplica las oportunidades de los delincuentes.

El ciberterrorismo y en particular el Yihadista, se aprovechan de la existencia del ciberespacio para magnificar sus ataques y se ha convertido en la mayor pesadilla para la seguridad de las naciones occidentales; tiene unas características tan amplias y destructivas que exigen una respuesta inmediata, contundente, unida, continuada e incansable de las naciones.

Nacen tantas amenazas desde cualquier lugar del mundo, la mano es tan larga y puede ser tan destructiva, que los estados deben responder a tantos frentes y tan rápido, que de no hacerlo, se podrían causar daños humanos, sociales y económicos irreparables.

Los países despiertan y reaccionan ante la gran amenaza; primero se trata de crear normativa y legislación al respecto, que deberá estar en continua actualización, para de esta forma poder combatirla respetando todos los derechos y valores que sostienen al mundo civilizado.

SEGUNDA: Estamos ante un terrorismo novísimo, transformado por internet y por la irrupción del Estado islámico. “Se trata de un fenómeno patológico a veces irracional, que habla en muchos idiomas por lo que para combatirlo es imprescindible la colaboración internacional. Un yihadista puede ser un individuo

de cualquier raza o color con raíces no identificables, agrupados militarmente y organizados entre ellos gracias a la nuevas tecnologías de la comunicación: INTERNET".

Podemos afirmar que la coordinación y cooperación entre naciones, es la peor pesadilla contra el terrorismo y de forma concreta contra el ciberterrorismo. Si todos los países estuvieran unidos en una misma organización o red que pudiera disponer de los mismos medios coordinados entre sí, este tipo de delitos serían mucho más difíciles de cometer.

TERCERA: La aparición de Internet tiene un papel protagonista y fundamental en la nueva orientación de los terroristas a la hora de captar, entrenar miembros, financiar y organizar. La posibilidad de colgar contenidos en una plataforma fácilmente accesible y sujeta a pocas censuras ha conllevado la aparición de manuales electrónicos en los que se explica detalladamente cómo y dónde adoctrinarse e instruirse para cometer actos terroristas. Este fenómeno se denomina "universidad abierta para la yihad".

Es posible decir que sin internet el terrorismo yihadista estaría mucho menos activo y expandido, y en consecuencia, por supuesto, sería mucho más controlable.

La fase más peligrosa para la captación de adeptos ala*yihad* es la fase de radicalización que permite a muchos jóvenes musulmanes ir desarrollando una postura positiva hacia el Islam radical. Podría decirse que el arma más importante para la radicalización es internet a través de chats, ciber-cafés, páginas web, etc. La lucha debe ir dirigida a arrasar la ideología: se pretende atacar directamente sobre el comportamiento adulterado, criminal y radical de los Yihadistas y nunca contra la idea real y pacífica del islam.

CUARTA: Organismos y naciones llegan a la misma conclusión: dejar sin financiación al terrorismo. Sino matarlo, es enjaularlo. Un terrorismo sin fondos es un terrorismo débil y decadente. Por este motivo las naciones se unen a través del

GAFI para combatir en principio el narcotráfico y más tarde también el terrorismo. En España se creó el SEPBLAC como una unidad ejecutiva de inteligencia financiera encargada de la lucha contra el blanqueo e infracciones de capital en España. Su regulación está recogida en los artículos 45-47 de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, determinando esta misma ley los 26 tipos de sujetos obligados a cumplir con esta normativa.

España como ejemplo descrito, cuenta con experiencia de años en el marco terrorista (las desarticuladas ETA y GRAPO), unas líneas estratégicas y unos marcos de cooperación con la UE, OTAN y la comunidad internacional, que son imitables y que le permiten defenderse contundentemente dentro de sus fronteras.

QUINTA: El ciberespacio juega un papel muy importante en las relaciones entre las naciones, pudiéndose convertir en uno de los principales escenarios de conflictos internacionales.

SEXTA: Son los países desarrollados los primeros en reaccionar contra los delitos cibernéticos. Alemania y EE.UU. en el año 1986 formalizan sus primeras actas y normativas. A partir de aquí empiezan a movilizarse los países. Los menos desarrollados despiertan forzados por el voraz riesgo, a principios-mediados de la década de los noventa. Muchos países son todavía vulnerables al ataque de un *hacker*. Una de las principales vías para combatir el ciberterrorismo y aumentar la seguridad en Internet es armonizar y estandarizar las leyes nacionales. Este método permitiría en principio, reducir la impunidad y evitar desigualdades en la prevención y persecución, sea cual sea el Estado donde se produzca el ataque.

En la actualidad, España, como país miembro de la Unión Europea, ve sometida su actuación legislativa a la regulación que de algunas materias se impone por parte de la Unión. Una de ellas es la creación de una sociedad de la información más segura, estableciendo las directrices para legislar los delitos informáticos y decidir cuáles son de ámbito Penal. El Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001, es una de las

herramientas de partida fundamentales del Derecho internacional. La meta de la Unión Europea es la consecución del ciberespacio como un espacio de libertad, seguridad y justicia.

SÉPTIMA: Uno de los objetivos de la estrategia de ciberseguridad, es poder legislar sobre todos los delitos que se cometen en este nuevo espacio delictivo del "ciberespacio" donde no hay fronteras, ni limitaciones en cuanto al poder de la acción basado en el anonimato, al alcance de todos y con gran repercusión social y mediática, pero ejercido siempre dentro de la búsqueda de justicia, eficacia y respeto a los derechos humanos.

Una vez determinados los nuevos delitos y sus penas, se puede afirmar que las leyes deben estar atentas a los cambios constantes de las amenazas, porque de no hacerlo los delincuentes sacarían un gran partido de ello. Así la UE y sus estados, siguen la línea de estandarizar todo lo posible los delitos y sus propias legislaciones antiterroristas, para en consecuencia poder combatir de forma compacta y unida este fenómeno denominado ciberterrorismo que puede alterar la economía de los países, sus empresas, infraestructuras y lo más importante, alterar el sueño, la tranquilidad y la paz social (estado del bienestar) de los habitantes de los países que lo sufren.

Si se establece un mecanismo de control, actualización y estandarización de las leyes contra los delitos cibernéticos, se construirá una de las bases para la lucha contra el ciberterrorismo. Debemos tener el control, siendo el ciberespacio el espacio más difícil de controlar.

OCTAVA: Estandarización de las leyes, la estrategia más importante para combatir el ciberterrorismo, que siguió, sigue y seguirá primando los esfuerzos de la comunidad internacional, es la estrategia de unificar las normas al respecto.

Fue la ONU en su lucha contra la cibercriminalidad, la que estableció una política mundial para la prevención de los crímenes "en línea". Posteriormente se estableció en Budapest la Convención sobre la Cibercriminalidad, participando el

Consejo de Europa en la protección de datos de carácter personal, desarrollándose un estudio por parte de la Unión Europea de las diferentes convergencias y perspectivas de la cibercriminalidad en el mundo, pero en ninguno de ellos se consiguió una homogenización de leyes, lo que atrae a la cibercriminalidad y desde el punto de la vista del Organismo de Cooperación de Desarrollo Económico (OCDE) está afectando en consecuencias económicas gravísimas.

NOVENA: Tanto las directivas europeas como las modificaciones realizadas recientemente en el Código Penal español en materia de terrorismo, están encaminadas a prevenir y minimizar los actos terroristas y sus consecuencias. En esta línea se han tipificado algunos delitos (*hacking*, *grooming*...) y se han aumentado las penas de otros, muchos de ellos relacionados con internet, dado que para los ciberdelincuentes, es su medio eficaz de adoctrinamiento, financiación, expansión y comisión de delitos así como medio de exaltación de sus logros y el ataque y humillación a las víctimas, (La directiva 2012/29/UE del Parlamento Europeo y del Consejo del 25 de Octubre del 2012, presta gran atención a las víctimas) e incluso se han puesto penas adicionales por cometer delitos tipificados anteriormente pero cometidos por internet (como la captación, exaltación, *bullying*, etc…). Son cuatro las conductas importantes estudiadas bajo el nombre de resoluciones manifestadas: la conspiración, la proposición, la provocación y la apología como forma de provocación. La Justicia las analiza y estudia y en base a su nueva percepción sumado a las nuevas condiciones del mundo actual (Internet, terrorismo, ciberterrorismo,…) lo toma como base en la última actualización de las leyes tanto penales como civiles "responsabilidad civil *exdelito*".

Podemos decir que con la última modificación del Código Penal, se amplía la prospectiva legal del terrorista como perteneciente a banda armada y se añade la figura del terrorista individual.

DÉCIMA: De forma paralela al análisis legislativo y hablando ya de las directrices defensivas, el primer tiempo de la aparición del ciberdelitos fue realmente desbordante; aparecían continuamente nuevas formas o sistemas de ataque y las naciones se organizaron, apareciendo gran cantidad de organismos, tratados y estrategias para combatir este nuevo fenómeno, todas ellas basadas en 4 pilares: prevención, protección, persecución y respuesta.

Tras nuestro análisis, podemos intuir que para el éxito en la lucha contra el ciberterrorismo, no sirve un sistema de defensa nacional simple y convencional. Además de la tecnología más moderna, se necesita un conjunto de sistemas de defensa que a su vez se unan a otros, creciendo según aumentamos fronteras, lo que nos hace concluir que la ciberdefensa es un gran entramado mundial de sistemas defensivos. La UE y la OTAN tratan de marcar las directrices de esta lucha en Europa.

Tras el análisis conjunto de toda la información recopilada en este estudio podemos afirmar que apoyado en la ley, el mundo civilizado ha creado un gran sistema u organigrama defensivo que crece, actualizándose continuamente, en medios económicos, humanos y tecnológicos para poder mantenerse efectivo y contrarrestar el poder destructivo de los ciberdelincuentes.

DECIMOPRIMERA: El mundo necesita una nueva y más fuerte regulación del ciberespacio, más estricta, organizada, estandarizada y sobre todo que cubra la totalidad del espacio cibernético. La autorregulación del ciberespacio solo cumple las expectativas a corto y medio plazo y solo podría valer a largo plazo en el caso que los Estados y la comunidad internacional, a través de expertos Juristas relacionados con la TIC, alcancen acuerdos globales para marcar las pautas legales de este.

DECIMOSEGUNDA: Las líneas estratégicas en ciberdefensa se basan en la investigación de los delitos, incremento de las infraestructuras, calidad de las redes y sistemas de información, mejora continuada de la tecnología, capacitación de profesionales…, en definitiva en implantar una cultura de ciberseguridad sólida

y sobre todo una intensa colaboración internacional que en los países más avanzados se plasma en lo que denominamos estrategia de ciberseguridad.

La Ciberdefensa no debe ser una actividad aislada sino que debe contemplarse dentro de las Estrategias de Seguridad Nacional, la Protección de Infraestructuras Críticas y en la Lucha contra Organizaciones Terroristas y Criminales.

España cuenta con un amplio, desarrollado, experimentado y controlado plan de estrategias, organismos y medios en ciberseguridad-terrorismo, operativo dentro de sus fronteras que a su vez se nutre de la colaboración con otros países y organizaciones internacionales, siendo el ECHELON la organización más potente del mundo en infraestructuras, medios económicos, humanos, tecnológicos y operativos en materia de espionaje y ciberseguridad, dirigida por las naciones anglosajonas y con la que España colabora de forma permanente para de esta forma alcanzar el éxito en sus actuaciones.

DECIMOTERCERA: Las Estrategias de Seguridad Nacionales y dentro de estas la parte especializada en ciberdefensa, son indispensables para organizar y llevar a cabo la defensa de las naciones y sus habitantes siempre haciendo prevalecer la defensa de la libertad, legalidad y el respeto por los derechos humanos. Si los países no contaran con ellas su defensa sería un caos, traduciéndose en un resultado catastrófico. España cuenta con una Estrategia de Seguridad Nacional y Ciberseguridad totalmente actualizadas que puede servir de ejemplo e inspiración para otros países.

Estas estrategias creadas dentro de la ley por los órganos legislativos de los Estados, deben de facilitar la colaboración y sincronización de todos los medios estructurales, tecnológicos, humanos y de inteligencia de que dispone un país para su defensa a todos los niveles y sobre todo deben de estar optimizándose y actualizándose continuamente para mantener siempre su efectividad.

DECIMOCUARTA: La Seguridad Nacional es definida de diferentes maneras según las diferentes naciones del mundo. Para las naciones que cuentan con abundantes recursos, la seguridad es regularmente la habilidad de protegerse contra los riesgos conocidos; la aplicación máxima de la tecnología, medios humanos y científicos contra las intenciones delictivas, lo que se traduce en inversión de medios económicos.

DECIMOQUINTA: Tras el estudio intrínseco de diversas sentencias homogéneas (tratan de los mismos delitos) de carácter terrorista, pero unas dictadas antes y otras después de la modificación en 2015 de la ley sobre materia terrorista hemos concluido:

En las modificaciones 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 se aumentan los delitos y las penas de éstos. Sin embargo, en las sentencias analizadas sobre delitos particulares como enaltecimiento del terrorismo o pertenencia a organización terrorista vemos que las penas impuestas por los jueces antes de la modificación suelen ser mayores o iguales que después. Podríamos decir que aunque de forma teórica o legislativamente se ha endurecido la actuación y directriz contra los delitos de carácter terrorista, judicialmente y en la práctica los resultados de las sentencias y en consecuencia sus penas se han mantenido o suavizado en la mayoría de los casos:

- Sentencia I - 2007: Delito de integración en organización terrorista islámica. (Sentencia de 10 años de cárcel y 10 años de inhabilitación).

- Sentencia II - 2007: Delito de integración en organización terrorista islámica. (Sentencia de 6 años de cárcel y 6 años de inhabilitación).

- Sentencia III - 2008: Delito de integración en organización terrorista islámica. (Sentencia de 9 años de cárcel y 10 años de inhabilitación). Delito de dirigir organización terrorista islámica. (Sentencia de 14 años de cárcel y 15 años de inhabilitación).

- Sentencia IV - 2012: Delito de integración en organización terrorista islámica. (Sentencia de 6 años de cárcel y 10 años de inhabilitación).
- Sentencia V - 2014: Apología del terrorismo. (Sentencia de 2 años de cárcel y 10 años de inhabilitación).
- Sentencia VI - 2017: Apología del terrorismo. (Sentencia de 1,6 años de cárcel y 8 años de inhabilitación).
- Sentencia VII - 2017: Delito de integración en organización terrorista islámica. (Sentencia de 10 años de cárcel y 18 años de inhabilitación). Delito de dirigir organización terrorista islámica. (Sentencia de 12 años de cárcel y 20 años de inhabilitación).

DECIMOSEXTA: Después del análisis de campo, podemos ver que los agentes de las fuerzas de seguridad coinciden en gran medida, en encontrarse con obstáculos legales a la hora de poder realizar sus actuaciones antiterroristas con éxito. Siguiendo en la línea de campo tras la encuesta realizada a jueces denotamos, que éstos, como es su cometido, abogan hacia el estricto cumplimiento del derecho a la intimidad, expresión y defensa de todos los derechos fundamentales de cualquier ciudadano.

Después de todos los actos terroristas acometidos últimamente (Barcelona, Paris, Niza, Londres, Estocolmo....) y concretamente el atentado del 22-05-2017 en la ciudad de Manchester, atentado realizado durante un espectáculo musical, dirigido a un público muy joven que nada sabe de guerras ni doctrinas religiosas y encaminado a crear un alto grado de terror, pánico e inseguridad entre la población, podemos recapacitar y decir: “nos encontramos aquí con una línea imaginaria de donde empiezan los derechos de uno y donde terminan los del otro”. No sabemos dónde colocar esta línea, probablemente deberían ser los ciudadanos, en un referéndum los que decidieran si prefieren más derechos o más seguridad. Si los ataques terroristas se siguen sucediendo es probable que la UE y sus estados se vean obligados a realizar una consulta al respecto. Al fin y al cabo son los ciudadanos los que al igual que deben acatar y cumplir las leyes, son

también los que tienen derecho a decidir dónde colocar esta línea, y como indica THERESA MAY: "necesitamos que se revise la legislación antiterrorista por considerarla demasiado tolerante hacia el extremismo", además, "para asegurarse que la policía y los servicios de seguridad cuenten con todos los poderes que necesiten para actuar de forma efectiva", regular el ciberespacio y en definitiva los actos terroristas.

DECIMOSÉPTIMA: ¿Son suficientes o están bastante especializados los Jueces en ciberdelitos? Como es sabido, son los jueces de la Audiencia Nacional los encargados de juzgar los delitos sobre terrorismo o ciberterrorismo, estando altamente especializados para ello, pero ¿son suficientes o llegan con la máxima efectividad a cualquier rincón de España? Puede que en estos momentos estén desbordados y en consecuencia podrían llegar a ser más efectivos.

Hemos observado con respecto a los jueces que juzgan los demás ciberdelitos en las diferentes salas penales del país, que no han recibido formación al respecto y al no existir amplia y añeja jurisprudencia se encuentren ante problemas de compleja resolución.

PROPUESTAS

La evolución seguida por los estados desarrollados o del denominado primer mundo, frente al fenómeno del ciberterrorismo es positiva y satisfactoria anunque no suficiente. Este tipo de defensa no es estática. Es totalmente dinámica, lo que se traduce en un no parar de aprendizaje, actuaciones, organización y cooperación.

Las naciones más desarrolladas y por lo tanto, las más sensibles al fenómeno, deben seguir trabajando en la linea actual; además deben desarrollar sus políticas y actuaciones sobre todo en los países menos preparados, donde los delincuentes se atrincheran para realizar sus acciones delictivas o ataques. Es aquí donde se debe invertir para de ésta forma no dejar vacíos que sirvan de cobijo a los criminales. Esto podemos conseguirlo incrementando la cooperación entre países, intentando equilibrar las diferencias defensivas entre unos y otros, lo que delimitará mucho a los delincuentes y sus acciones.También permitirá darles alcance con mayor facilidad y sobre todo limitará la posibilidad y el número de delincuentes, actuaciones y en definitiva catástrofes terroristas.

Además de crear estrategias, métodos y resultados efectivos y positivos contra el ciberterrorismo en los países occidentales, debemos hacer lo mismo en los países más pobres, porque los delincuentes encuentran cobijo en las naciones subdesarrolladas con menos seguridad desde donde facultados por la naturaleza del ciberespacio pueden actuar y esconderse. Debemos suministrar e implantar estos métodos defensivos en estos países menos favorecidos, intentando de esta forma crear una red mundial de seguridad que actúe con niveles similares en todos los rincones del planeta, no dejando espacio sin ley a los ciberdelincuentes.

Además debemos unirnos contra los países y naciones que no entren a formar parte de esta red, ya que estos países sirven de refugio para los delincuentes del ciberespacio; incluso muchas veces son los mismos países los que de forma encubierta realizan ataques a otros estados por intereses propios, estratégicos de tipo ideológico, económico o militar.

España debe seguir en la línea creciente de desarrollo anticiberterrorista siguiendo los marcos de la UE y de la OTAN, siendo la UE la que debiera reforzar sus presupuestos, estrategias y acciones defensivas dentro de sus fronteras, incrementando sus sinergias y evolucionando hacia una unión cada vez más fuerte y conjunta de sus estados miembros, dando siempre una imagen al exterior de un solo bloque.

La Unión Europea debe utilizar su potencial tecnológico, económico y social con respecto al resto del mundo. De esta forma y aprovechándose de su PIB conjunto, que es unos de los mayores del mundo, le facilitará la tarea de crear instituciones, habilidades, tecnología y estratégicas únicas y homogéneas para todos los estados miembros, incluso si en el futuro fuera necesario crear un único y potente ejército que le permita defenderse y ser respetada por todas las demás naciones del planeta para poder llevar a cabo con éxito sus políticas sociales, económicas y de seguridad dentro del marco que identifica a la UE, del respeto al ser humano y sus derechos fundamentales.

BIBLIOGRAFÍA

AUTORES

ABAD ARRANZ, M. Á. (2016). Capacidades de ciberseguridad en España. .En Martín Minguijón, A. R. y Morán Martín, R. (Coords.) Seguridad, Extranjería y otros estudios histórico-jurídicos (pp. 145-154). Madrid: Iustel.

ABELLÁN, L. (5 de septiembre de 2014). EE UU forja una alianza de 10 países para combatir a los yihadistas. *El Pais*. Recuperado de:http://internacional.elpais.com/internacional/2014/09/05/actualidad/1409917501_927947.html

ACURIO DEL PINO, S. (2011). Delitos informáticos: Generalidades. (OEA) Jurídica Cono Sur. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

AGUDO FERNÁNDEZ, E., PERRINO PÉREZ, Á. L., Y JAÉN VALLEJO, M. (2016). Terrorismo en el siglo XXI. La respuesta penal en el escenario mundial. Madrid: Dykinson.

ALSEDO, Q. Y HERRÁIZ, P. (31 de agosto de 2017). Sombras y errores de la investigación de los atentados de Barcelona y Cambrils*. El Mundo, Madrid.* Recuperado de: http://www.elmundo.es/cataluna/2017/08/25/599f2c56e5fdeab0598b4641.html

ALDECOA LUZARRAGA, F. Y GUINEA LLORENTE, M. (20 de febrero de 2008). El rescate sustancial de la Constitución Europea a través del Tratado de Lisboa: la salida del laberinto. Documento de Trabajo nº 9, Real Instituto Elcano. Recuperado de:

http://www.realinstitutoelcano.org/wps/portal/europe/europa/home/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jjEBf3QG93QwMLLxMjA08jQxNDf0dTo1BjQ_2CbEdFAMD4gFE!/?WCM_PORTLET=PC_7_3TDGQKG108N000I2HUKBMI2OG3000000_WCM&WCM

ALONSO GARCÍA, J. (2015). Derecho penal y redes sociales (1ª ed.). Madrid: Aranzadi.

ÁLVAREZ PASTOR, D. Y EGUIDAZU PALACIOS, F. (2006). Manual de prevención del blanqueo de capitales. Barcelona: Marcial Pons, Ediciones Jurídicas y sociales, S. A. Recuperado de: https://www.marcialpons.es/static/pdf/100788061.pdf

BALLÉN, M. PULIDO, RODRIGO Y ZÚÑIGA, FLOR. (2007). Abordaje hermenéutico de la investigación cualitativa. Teoría, proceso, técnicas. Universidad coorporativa. Facultad de Derecho. Bogotá, Colombia. Segunda edición. ISBN: 958-8325-24-8. Recuperado de: https://books.google.com.co/books?id=B2L6wakmpIwC&printsec=frontcover&dq=abordaje+hermeneutico&hl=es&sa=X&ved=0ahUKEwjWxpyB0-nNAhXLGx4KHedgBVcQ6wEIHTAA#v=onepage&q=abordaje%20hermeneutico&f=false

BLANCO NAVARRO, J. M. (2016). Exdirector del centro de Analisis y Prospectiva de la Guardia Civil (CAP). Foro para la paz en el mediterraneo, recuperado de: https://www.uma.es/foroparalapazenelmediterraneo/?p=5741

_____. (7 de septiembre de 2011). Seguridad e inteligencia 10 años después del 11-S. Documento Marco del Instituto Español de Estudios Estratégicos (ieee). Recuperado de: http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM09-2011SeguridadInteligencia.pdf

BONILLA, ELSSY & RODRÍGUEZ, PENELOPE. (1997). Más allá del dilema de los métodos. 2 ed. Bogotá. Colombia. ISBN: 958- 9057-72-1.

CABULI, E. Y JATIB, G. J. (2 de mayo de 2006). La prevención del lavado de activos y el ejercicio profesional en el mundo globalizado. *Revista La Ley*. Recuperado de: https://www.colegio-escribanos.org. Ar/biblioteca/cgi-bin/ESCRI/ARTICULOS/48676.pdf

CANDAU ROMERO, J. (2011). Estrategias nacionales de ciberseguridad. Ciberterrorismo. Cap. VI. En IEEE, Instituto Español de Estudios Estratégicos, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Cuaderno de seguridad nº 149* (pp. 259-322). Madrid: Ministerio de Defensa. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

CANO PAÑOS, M. Á. (2008). Internet y terrorismo islamista. Aspectos criminológicos y legales. *EGUZKILORE Cuaderno del Instituto Vasco de Criminología* nº 22, pp. 67-88. Recuperado de http://www.ehu.eus/documents/1736829/2176658/03+Cano.indd.pdf

CARLINI, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. Instituto Español de Estudios Estratégicos. Madrid: IEEE. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

CARO BEJARANO, M.J. (17 de marzo de 2011). Nuevo concepto de ciberdefensa de la OTAN. Documento informativo del IEEE-09/2011. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

CASTAÑÓN ÁLVAREZ, M. J. (2012). Protección penal de las víctimas en los delitos de terrorismo. Tesis Universidad Complutense de Madrid, Facultad de Derecho. Recuperado de: http://eprints.ucm.es/16562/1/T33973.pdf

CERNUDA, O. (15 de junio de 2001). Ciberespionaje: ¿ECHELON contra ETA? *Periódico digital navegante.com*. Recuperado de: http://www.elmundo.es/navegante/2001/06/15/esociedad/992605466.html

CHICHARRO LÁZARO, A. (2013). La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo. En La Sociedad Ruido: Entre El Dato y El Grito. *Cuadernos artesanos de comunicación.* (53), 80-81.

_____. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *Revista de Internet Derecho y Política IDP*. (9). Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3101795

CHICOTE, J. (4 de septiembre de 2017). El imán de Ripoll, relacionado con el atentado contra el cineasta Theo van Gogh*, ABC* España, Madrid.Recuperado de: http://www. Abc.es/espana/abci-iman-ripoll-relacionado-atentado-contra-cineasta-theo-gogh-201709042148_noticia.html

COLOM, G. Y FOJOM, E. (6 de julio de 2016). Nuevo paso de la OTAN en ciberdefensa. *Periódico digital El Español.* Recuperado de: http://www.elespanol.com/opinion/20160705/137856215_12.html

CONWAY, M. (2003). "Terrorism and IT: Cyberterrorism and Terrorism Organisations Online", Paper presented at the International Studies Association (ISA) Annual International Convention, Portland; recuperado de: www.firstmonday.org/issues/issue7_11/conway /index.html

CORONADO CONTRERAS, J. E. (7 de febrero de 2015). Breves consideraciones sobre la ciberdelincuencia y el ciberterrorismo. *Unión de Revistas de Estudiantes de Derecho URED.* Recuperado de http://www.ured.org.mx/ured/breves-consideraciones-sobre-la-ciberdelincuencia-y-el-ciberterrorismo/

DEL ROSAL BLASCO, B. (2009). ¿Hacia el derecho penal de la postmodernidad? *Revista Electrónica de Ciencia Penal y Criminología.* Núm. 11,08:1-08-64. Recuperado de:http://criminet.ugr.es/recpc/11/recpc11-08.pdf

ECKSTEIN, H. (1965). On the Etiology of Internal Wars. (ed.), Internal War (New York: The Free Press.

FERNÁNDEZ, R. (30 de mayo de 2009). Estonia, primera víctima de los hackers. *El País.* Recuperado de: http://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

FERRERES MUÑOZ, A. (2016). Intervencion en el ciberbullying: Menores en las redes. Trabajo Fin de Grado Universitat Jaume I. Recuperado de: http://repositori.uji.es/xmlui/bitstream/handle/10234/161202/TFG_2015_ferreresA.pdf?sequence=1&isAllowed=y

FONTES, J. (2018). Currículum profesional, con listado de sus publicaciones. Professor associado com agregaçao. *Observatorio Político*. Recuperado de: http://www.observatoriopolitico.pt/jose-fontes

GABARI GÁMEZ, A. (2015). La regulación del terrorismo en el CP: Una regulación de excepción. Trabajo Fin de Grado Universidad Pública de Navarra. Recuperado de: http://academica-e.unavarra.es/bitstream/handle/2454/18400/72249TFGGabari.pdf?sequence=1&isAllowed=y

GARCÍA, J. (2014). Análisis de los elementos esenciales de la actual estrategia de seguridad nacional, y su comparativa con su predecesora de 2011 y con las estrategias de seguridad nacional de nuestro entorno. Instituto Universitario Gutiérrez Mellado. Madrid.

GARCÍA, T. (2016). Enaltecimiento: de la pancarta al Twitter. *Periódico digital diagonalperiodico.net.* Recuperado de: https://www.diagonalperiodico.net/libertades/29391-enaltecimiento-la-pintada-al-twitter.html

GIBSON, W. (2004). Pattern Recognition/Mundo espejo. Versión española. Minotauro.

GIL NAVALON, R. (2012), El vacío legal del ciberespacio, *"Revista de Aeronáutica y Astronáutica*", Jefe de la unidad SEGINFOPER, INS y DOC (Área de Seguridad de la Información (SDGTIC).

GÓMEZ VIEITES, Á. (1 de agosto de 2014). La lucha contra el ciberterrorismo y los ataques informáticos. Ponencia X Reunión española sobre criptología y seguridad de la información, pp. 251-261. Recuperado de: http://www.edisa.com/wp-content/uploads/2014/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

GONZÁLEZ, M. (5 de febrero de 2015). "España es, tras EE.UU. y Reino Unido, el país que sufre más ciberataques. El País. Recuperado de: http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html

GONZÁLEZ HURTADO, J. A. (2013). Delincuencia informática: Daños informáticos del articulo 264 del codigo penal y propuesta de reforma. Tesis doctoral. Universidad Complutense de Madrid, Facultad de Derecho. Recuperado de: http://eprints.ucm.es/23826/1/T34976.pdf

GUTIÉRREZ, A. (18 de agosto de 2016). Quiénes son y cómo se enrolan los yihadistas. *Periódico digital proceso.com.* Recuperado de: http://vlex.com/vid/enrolan-yihadistas-647106597

HIDALGO PÉREZ, M. (19 de diciembre de 2017). Seguridad. España tiene perdida la guerra contra el cibercrimen. *El País*, Madrid. Recuperado de: https://retina.elpais.com/retina/2017/07/11/tendencias/1499762151_884595.html

IBERTI, J. (2001). Violencia y escuela. Medidas y propuestas concretas. Paidós.

JUNCKER, J-C. (2017). European Commission. *State of the Union Address*, (13 September 2017), Cibersecuriy tackling non-cash payment frau, page 1, Brussels.

LABORIE IGLESIAS, M. (3 de junio de 2014). La estrategia de seguridad nacional (mayo 2013). Instituto Español de Estudios Estratégicos. Madrid: IEEE. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA34-2013_EstrategiaSeguridadNacional-2013_MLI.pdf

LLORENTE, A. (20 de diciembre de 2010). La cooperación judicial antiterrorista entre España y Marruecos. ARI, Real Instituto El Cano, España. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari174-2010

LÓPEZ GARCÍA, L. Y. (2016). Proyecto estratégico de prevención de la cibercriminalidad para México en la globalización (una mirada desde el extranjero). Facultad de derecho y ciencias sociales - división de estudios de posgrado. México.

LÓPEZ ZAMORA, P. (2006). El ciberespacio y su ordenación, Capítulo 2: Regulando el ciberespacio, Difusión jurídica y temas de actualidad, p. 95, recuperado de: http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

MARCOS MARTÍN, T. (2017). *Radicalism and terrorist in the 21st century, Legal Instruments and Specific Actions in the EU's Fight against Terrorism*, p. 248.

MARTÍN DE POZUELO, E. (19 de abril de 2015). El estado islámico capta terroristas en dos meses. *La vanguardia*. Recuperado de: http://www.lavanguardia.com/politica/20150419/54430030929/estado-islamico-capta-terroristas.html

MARTÍN MINGUIJÓN, A. R. y MORÁN MARTÍN, R. (Coords.) Seguridad, Extranjería y otros estudios histórico-jurídicos (pp. 145-154). Madrid: Iustel.

MARTÍNEZ DE SALAS Y SÁNCHEZ - Abogados. (2016). La captación terrorista. Recuperado de: http://www.martinezdesalasysanchez.com/noticias/2016/01/16/la-captacion-terrorista.html

MICHAEL N. SCHMITT, M.N. (ed). (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, p. 45.

MOURE COLÓN, F. (2014). *Armonización de las líneas de acción de la estrategia integral de seguridad de la comunidad internacional: aportación española* (pp. 391-396). Madrid: Dykinson.

OLVERA GORTS, M. (Junio de 2013). Ciencia, tecnología y Sociedad. Ciberterrorismo e infraestructuras críticas.

ORTIGOSA, Á., Y HERNÁNDEZ GARCÍA, L. F. (2016). Las nuevas amenazas cibernéticas del S.XXI Ciberterrorismo: Nueva forma de subversión y desestabilización. *En Cuadernos de La Guardia Civil, 75 Aniversario.* Servicio de Información de la Guardia Civil (pp. 104-122). Aranjuez: Centro Universitario de la Guardia Civil. Recuperado de http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/documents/18266_19488.pdf

PANIAGUA, E. (19 de mayo de 2017). Los políticos, perdidos ante la era digital. *El mundo* Economía, España. Recuperado de: http://www.elmundo.es/economia/2017/05/19/591e0a97ca4741a93d8b45c8.html

PASTOR ACOSTA, Ó., PÉREZ RODRÍGUEZ, J. A., ARNÁIZ DE LA TORRE, D. Y TABOSO BALLESTEROS, P. (2009). Seguridad nacional y Ciberdefensa. *Cuadernos Cátedra ISDEFE-UPM* nº 6. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.Recuperado

de:http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

PONCE, I. (17 de abril de 2012). Redes sociales. Historia de las redes sociales. Observatorio Tecnológico. Gobierno de España. Ministerio De Educación, Cultura y Deporte. Recuperado de Observatorio Tecnológico. Ministerio de Educación Cultura y Deporte: http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redes-sociales?start=2

PONTE, M. (2015). La reforma de los delitos de terrorismo mediante la ley orgánica 2/2015. Recuperado de: http://www.seguridadinternacional.es/?q=es/content/la-reforma-de-los-delitos-de-terrorismo-mediante-la-ley-org%c3%a1nica-22015

PRIETO OSÉS, R Y OTROS. (abril de 2013). Guerra cibernética: Aspectos organizativos. XXXIII curso de Defensa Nacional. CESEDEN. Madrid.

PUENTE GUERRERO, P. (2011). La regulacion de los delitos de terrorismo en la LO 5/2010 -¿son los terroristas nuestros enemigos?- especial referencia a la libertad vigilada. *Revista Derecho Penal Y Criminología*, 32, 83. Universidad Externado de Colombia. Recuperado de: http://revistas.uexternado.edu.co/index.php/derpen/article/view/3071/2844

RAMELSBERGER, A. (2008): Der Deutsche Dschihad.

RODRÍGUEZ BERNAL, A. (2007). Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia. *Revista de Derecho Informático* 103, pp. 1-42. Recuperable en: https://dialnet.unirioja.es/servlet/articulo?codigo=2248647

ROMEO CASABONA, C. M. (s.f.). El cibercrimen en el ámbito económico y patrimonial. Guía docente de la asignatura (pp. 1-14). Universidad del País Vasco.

ROVIRA DEL CANTO, E. (2011). Nuevas formas de ciberdelincuencia intrusiva: el hacking y el *grooming*. *Iuris*: Actualidad y práctica del derecho, (160), pp. 36-44.

ROY, O. (2003). El islam mundializado. Los musulmanes en la era de la globalización (Trad. por José Ramón Monreal), Barcelona: Ediciones Bellaterra.

RUIZ DÍAZ, J. (22 de octubre de 2016). Ciberamenazas: ¿el terrorismo del futuro? Instituto Español de Estudios Estratégicos. Madrid: IEEE. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

SÁNCHEZ FRÍAS, A. (2016) ¿Cazador o presa en la telaraña del terror? La UE en la lucha contra el ciberterrorismo. Universidad de Málaga. Recuperado de: https://riuma.uma.es/xmlui/bitstream/handle/10630/12586/Ponencia%20UC3M%20Alejandro%20Sanchez%20Frias.pdf?sequence=3

SUBIJANA ZUNZUNEGUI, I. J. (diciembre de 2008). El ciberterrorismo: una perspectiva legal y judicial. *Eguzkilore Cuaderno del Instituto Vasco de Criminología.* (22), pp. 169-187. Recuperado de http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

THEVESSEN, E. (2005). Terroralarm. Deutschland und die islamistische Bedrohung. Pp. 82 y ss. Berlín: Rowohlt.

TRAVIS, A. (4 de junio de 2017). THERESA MAY recupera su discurso contra el extremismo que hasta ahora no había aplicado en el Gobierno, *The Guardian*, *www.eldiario.es*, Londres. Recuperado de: http://www.eldiario.es/theguardian/atentado-Londres-May_0_650935283.html

TRUJANO RUIZ, P., DORANTES SEGURA, J., Y TOVILLA QUESADA, V. (2009). Violencia en internet: Nuevas victimas, nuevos retos. *Liberabit,* Vol 15 nº 1, pp 7-19. Universidad Nacional Autónoma de México. Recuperado de: http://132.248.9.34/hevila/Liberabit/2009/vol15/no1/1.pdf

URUEÑA CENTENO, F. J. (2015). Ciberataques, la mayor amenaza actual. Documento de Opinión nº 09/2015. Instituto Español de Estudios Estratégicos. Madrid: IEEE.

VALLES CAVIAS, J. A. (2017). El concepto de acto terrorista y el comportamiento de fuerzas armadas durante un conflicto armado. Comentario de la sentencia TJUE (Gran Sala) de 14 de marzo de 2017, asunto C-158/14. Revista de Derecho Comunitario Europeo, 57, 689-707. Recuperado de: https://doi.org/10.18042/cepc/rdce.57.09

VÁZQUEZ LIÑÁN, M. (2000). La propaganda de guerra en Internet: el caso chechenio. *Revista Historia y comunicación Social*, nº 5 pp. 53-74. Universidad Complutense de Madrid. Recuperado de: http://revistas.ucm.es/index.php/HICS/article/view/HICS0000110053A/19545

VILLARREAL, R. (24 de agosto de 2017), El 'héroe de Cambrils', instruido en Melilla, *El Mundo* Catalunya, Tarragona. Recuperado de: http://www.elmundo.es/cataluna/2017/08/24/599dec79e2704ea87f8b460b.html

WESSING, T. (16 de agosto de 2017). The German IT Security Law. Lexology. Recuperado de: https://www.lexology.com/library/detail. Aspx?g=9368f280-b504-4914-8850-30ca58774e00

YÁRNOZ, C. (13 de enero de 2015) Valls anuncia controles inmediatos sobre internet en la lucha antiyihadista. *El País*. Recuperado de:http://internacional.elpais.com/internacional/2015/01/13/actualidad/1421145961_694800.html

ZEA PASQUÍN, F. (Marzo 2013). Ciberdefensa Militar.*Revista Española de Ciberdefensa.* Núm 293. pp. 48-40. Recuperado de:http://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-293-ciberdefensa.pdf

ZULOAGA, J.M. (19 de agosto de 2017) ¿Qué pasó en Alcanar? Los Mossos no avisaron a la Guardia Civil. *La Razón*. Madrid. Recuperado de: http://www.larazon.es/espana/que-paso-en-alcanar-los-mossos-no-avisaron-a-la-guardia-civil-ON15814587

BIBLIOGRAFÍA

INSTITUCIONES/ORGANISMOS

ABC NEWS. (21 de mayo de 2017). North Korea's Unit 180, the cyber warfare cell that worries the West, Australia. Recuperado de: http://www. Abc.net. Au/news/2017-05-21/north-koreas-unit-180-cyber-warfare-cell-hacking/8545106

AGENCIA EFE. (31 marzo 2018). España registra en 2 meses mas incidentes de ciberseguridad que en todo el 2014. *El Mundo.* Madrid. Recuperado de: http://www.elmundo.es/espana/2018/03/31/5abf4d9e268e3ebc098b4586.html

ANIMAL POLÍTICO. (23 de enero de 2017). Redacción. Detienen en España a una mexicana por el delito de enaltecimiento y promoción del terrorismo. *Periódico digital animalpolitico.com* Recuperado de: http://www. Animalpolitico.com/2017/01/detienen-espana-mexicana-la-acusan-difundir-propaganda-terrorista/

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA POLICÍA NACIONAL. (2017). BIT. Recuperado de: https://www.policia.es/org_central/judicial/udef/bit_alertas.html

BURBUJA. (9 de agosto de 2013). Echelon: la mayor red de espionaje del mundo. Recuperado de: https://www.burbuja.info/inmobiliaria/conspiraciones/449941-echelon-mayor-red-de-espionaje-del-mundo.html#

CAP. (abril de 2017). Centro de Análsis y Prospectiva, Guardia Civil. Boletín UE.

_____. (Enero de 2016). Centro de Análsis y Prospectiva, Guardia Civil.Boletín UE. Recuperado de: http://intranet.bibliotecasgc.bage.es/intranet-

tmpl/prog/local_repository/documents/17619.pdf

CCN. (2004). Centro Criptológico Nacional (CCN). Creado por RD 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). Recuperado de: https://www.ccn.cni.es/

CN-CERT IA-09 (Mayo de 2018). Centro Criptológico Nacional (CCN). Ciberamenazas y tendencias, Pág. 8. Recuperado de: https://lnkd.in/dHJa2uc

CERTSI (21 de octubre de 2015). Equipo de Respuestas ante Emergencias Informáticas de Seguridad e Industria. Acuerdo suscrito por Secretarías de Estado de Seguridad y de Telecomunicaciones y para la Sociedad de la Información. Recuperado de: https://www.certsi.es/

CIBERDERECHO (2015). El nuevo artículo 510 CP de España. Recuperado de: http://www.ciberderecho.com/el-nuevo-articulo-510-del-codigo-penal-de-espana/

COLEGIO DE ABOGADOS DE MADRID. (2015). Cuadro comparativo LO 1/2015. Recuperado de la tabla comparativa: http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

CNI. (2002). Centro Nacional de Inteligencia.Servicio de Inteligencia de España. Recuperado de:https://www.cni.es/

CNPIC.(2017). Centro Nacional para la Protección de las Infraestructuras y Ciberseguridad. Recuperado de: http://www.cnpic.es/Ciberseguridad/index.html

CONSEJO DE MINISTROS, ESPAÑA. (16 de julio de 2010). Acuerdo de la Estrategia 2011-2015 del Plan Avanza.

CONSEJO DE SEGURIDAD NACIONAL, ESPAÑA. (5 de diciembre de 2013). *Aprobada la Estrategia de Ciberseguridad Nacional de 2013.* Nota de prensa. Recuperado de https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

Consejo General del Poder Judicial. (17 de julio de 2008). Tribunal Supremo, sala de lo penal, sentencia nº 503, 2008, Recuperado de: http://www.poderjudicial.es/search/contenidos.

Action?action=contentpdf&databasematch=TS&reference=1458813&links=&optimize=20081002&publicinterface=true

CONSEJO UNIÓN EUROPEA. (25 de abril de 2017). Directiva sobre el control de la adquisición y tenencia de armas, que revisa y completa la Directiva 91/477/CEE. Recuperado de: http://www.consilium.europa.eu/es/press/press-releases/2017/04/25/control-acquisition-possession-weapons/

COLEGIO DE ABOGADOS DE MADRID. (2015). Cuadro comparativo LO 1/2015. Recuperado de la tabla comparativa: http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

DIARIO POPULAR. (4 de junio de 2017). Discurso Primera Ministra Británica. Recuperado de: https://www.diariopopular.com. Ar/internacionales/theresa-may-pidio-leyes-mas-duras-contra-el-terrorismo-n311117

EL ECONOMISTA. (17 de abrli de 2018). La ciberseguridad es la principal preocupación de los ejecutivos. Recuperado de: http://www.eleconomista.es/tecnologia/noticias/9078001/04/18/La-ciberseguridad-la-principal-preocupacion-de-los-ejecutivos-bancarios-segun-PwC.html

ELNACIONAL.ES. (24 de junio de 2015) ¿Cómo castiga el código penal la humillación a las víctimas del terrorismo? *Periódico digital elnacional.es* Recuperado de: http://www.europapress.es/nacional/noticia-castiga-codigo-penal-humillacion-victimas-terrorismo-20150624174852.html

EL PAÍS. (24 de mayo de 2017). Así te hemos contado el atentado en el Manchester Arena. España. El País. Recuperado de: https://internacional.elpais.com/internacional/2017/05/23/actualidad/1495496576_039320.html

ENTELGY. (2018). Blog Corporativo. Recuperado de: https://blog.entelgy.com/encuesta-ciberseguridad/

ESCUELA DE ALTOS ESTUDIOS DE LA DEFENSA. (Junio de 2014). Estrategia de la información y seguridad en el ciberespacio. Documentos de Seguridad y Defensa nº 60 Recuperado de:

https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf

EUROPEAN COMMISSION. (2018). Glossary and Acronyms. Recuperado de: http://ec.europa.eu/idabc/en/document/651/5892.html

_____. (2017). State of the Union. Cybersecurity EU Agency and Certification Framework, Brussels.

_____. (19 de septiembre de 2017). Press release: The Commission scales up response to cyberattacks, Brussels.

_____. (13 de septiembre de 2017). High representative of the unión for foreign affairs and security policy. Joint communication to the European parliament and the council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 8 and 9, Brussels.

_____. (Junio de 2017. Publicada en septiembre de 2017). Dirección General de Migración y Asuntos de Interior y coordinada por la Dirección General de Comunicación *Eurobarómetro especial 464ª*. Las actitudes de los europeos hacia la ciberseguridad, Bruselas.

_____. (25 de enero de 2017). *Fourth progress report towards an effective and genuine Security Union*. Recuperdo de: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20170125_4th_progress_report_on_the_security_union_en.pdf

_____. (2015). Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra el terrorismo, y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo.

_____. (7 de febrero de 2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Recuperado de: https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

EUROPEAN UNION. (Enero 2018). *Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. The European Union Agency for Network and Information Security (ENISA).* Recuperado de:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

_____. (junio de 2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. EU Open Data Portal. Recuperado de: https://data.europa.eu/euodp/data/dataset/S2171_87_4_464A_ENG

_____. (19 de julio de 2016). 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 en la Unión (Directiva sobre ciberseguridad NIS). Recuperado de: http://noticias.juridicas.com/base_datos/Admin/579387-directiva-2016-1148-ue-de-6-jul-medidas-destinadas-a-garantizar-un-elevado.html

_____. (22 de julio de 2015). EUR-Lex. Cooperaciones reforzadas. Recuperado de: https://es.wikipedia.org/wiki/EUR-Lex

_____. (25 de octubre de 2012). Parlamento.Directiva 2012/29/UE del Parlamento Europeo y del Consejo por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la decisión marco 2001/220/jai del consejo, 60. Recuperado de https://www.boe.es/doue/2012/315/l00057-00073.pdf

_____. (26 de octubre de 2005). Parlamento.DOUE nº 309, Directiva 2005/60/CE del Parlamento Europeo y del Consejo: relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo. Recuperado de: http://www.sepblac.es/espanol/legislacion/prevbcap/pdf/directiva_2005_60.pdf

_____. (15 de octubre de 2010). EUR-Lex. Tratado de Maastricht sobre la Unión Europea. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:xy0026

EUROPOL. (2013). European Cybercrime Centre (EC3). Recuperado de: https://www.europol.europa.eu/ec3

FATF (1986). The Financial Action Task Force, Grupo de Acción financiera Internacional. Recuperado de: http://www.fatf-gafi.org/

FBI. (2017). Federal Bureau of Investigation. Terrorismo.Recuperado

de:https://www.fbi.gov/investigate/terrorism

FEDERAL MINISTRY OF THE INTERIOR, GERMANY. (2011). Cyber Security Strategy for Germany. Recuperado de: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

ESYS. (2016). Fundación ESYS. Informe anual de la seguridad, p. 98. Madrid.Recuperado de: http://www.fundacionesys.com/es/system/files/INFORME%20ANUAL%20SEGURIDAD%20ESYS%202016_1.pdf

GABINETE DE COORDINACIÓN DE ESTUDIOS. (2016). Secretaria de Estado. Ministerio del Interior, Madrid.Gobierno de España. (23 de junio de 2010). Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP.

GOBIERNO DE PORTUGAL. (2015). National Cyberspace Security Strategy. Recuperado de: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf

GRUPO DE DELITOS TELEMÁTICOS DE LA GUARDIA CIVIL. (2017). GDT. Recuperado: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

GRUPO DE TRABAJO C-24. (2009). Derecho & cibercrimen. Internet: Un espacio para el cibercrimen y el ciberterrorismo. Recuperado de: http://www.cibersociedad.net/congres2009/es/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610

INCIBE. (Mayo de 2018). Instituto Nacional de Ciberseguridad. *Cibercrime: Concept, Types and State*.

_____. (27 de octubre de 2014). Instituto Nacional de Ciberseguridad de España. Acuerdo adoptado en Junta General. Recuperado de https://www.incibe.es/que-es-incibe

INSTITUTO DE DEFENSA NACIONAL, PORTUGAL. (Diciembre 2013). Cuaderno 12: Estrategia de Información y seguridad en el ciberespacio Investigación conjunta IDN-CESEDEN.

JEFATURA DEL ESTADO. ESPAÑA. (2 de julio de 1985) Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *Boletín Oficial del Estado (BOE)* núm. 157, de 2 de julio de 1985. Referencia: *BOE*-A-1985-12666. Consolidada 28 de octubre de 2015. Recuperado de: https://www.boe.es/buscar/pdf/1985/BOE-A-1985-12666-consolidado.pdf

_____. (17 de septiembre de 2010). Instrumento de ratificación del Convenio sobre Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. *Boletín Oficial del Estado (BOE)*. Núm. 226. Sec. I. pp. 78847-78896. Recuperado de: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

_____. (29 de abril de 2013). Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado (BOE-A-2010-6737)*, núm. 103., pp. 37458 a 37499.

_____. (29 de septiembre de 2015). Ley 36/2015 de 28 de septiembre, de Seguridad Nacional. *Boletín Oficial del Estado (BOE)*. núm. 233, pp. 87106-87117. Recuperado de: https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

JUICIOPENAL.COM (2015). Las resoluciones manifestadas: la conspiración, la proposición, la provocación y la apología. Recuperado de: https://juiciopenal.com/delitos/las-resoluciones-manifestadas-la-conspiracion-la-proposicion-la-provocacion-y-la-apologia/

MARCA ESPAÑA. (7 de abril de 2016). Cooperación hispano-marroquí contra el terrorismo, un modelo a seguir. www.marcaespaña.es. España. Recuperado de: http://marcaespana.es/actualidad/cooperaci%C3%B3n-hispano-marroqu%C3%AD-contra-el-terrorismo-un-modelo-seguir

MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES PÚBLICAS. (23 de enero de 2018). Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. *BOE* nº 20, sección, pág. 8186-90, Gobierno de España. Recuperado de: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-799.pdf

MINISTERIO DE DEFENSA. (19 de marzo de 2004). Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, para preservar la seguridad de los sistemas de las tecnologías de la información de la

Administración. *Boletín Oficial del Estado (BOE)* nº 68, pp. 12203-12204, Recuperado de:https://www.boe.es/boe/dias/2013/04/13/pdfs/BOE-A-2013-3907.pdf

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL. (2017). Agenda Digital para España. Recuperado de: http://www. Agendadigital.gob.es/agenda-digital/Paginas/agenda-digital. Aspx

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA. (29 de julio de 2017). Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. *Boletín Oficial del Estado (BOE)núm. 180, pp. 70439-70468.* Recuperado de: https://www.boe.es/boe/dias/2017/07/29/pdfs/BOE-A-2017-9013.pdf

MINISTERIO DE INDUSTRIA. ENERGÍA Y TURISMO. (22 de junio de 2012). Informe de recomendaciones del Grupo de expertos de Alto Nivel de la Agenda Digital para España. (pp. 51-52). Recuperado de http://www.minetur.gob.es/telecomunicaciones/es-es/novedades/documents/informe-recomendaciones-ade.pdf

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA, CHILE (2017). Política Nacional de Ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

MINISTERIO DEL INTERIOR, ESPAÑA. (28 de julio de 2017). El Ministerio del Interior modifica la estructura de la Policía Nacional y de la Guardia Civil para afrontar con mayor eficacia los nuevos retos de seguridad. Nota de prensa. Recuperado de: http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/7578978

_____. (2016). Anuario estadístico del Ministerio del Interior 2015. Recuperado de: http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2015.pdf/03be89e1-dd38-47a2-9ce8-ccdd74659741

MINISTERIO DE JUSTICIA, ESPAÑA. (19 de enero de 2008). Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE* núm. 17. Texto consolidado de 8 de marzo de 2012. Recuperado de: https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

MINISTERIO PÚBLICO, PORTUGAL. (2015). PGDL (Procuradoria-Geral distrital de Lisboa, Lei nº 60/2015 de 24 de junio que modifica la ley antiterrorista portuguesa.

_____. (2003). PGDL (Procuradoria-Geral distrital de Lisboa), Lei nº 52/2003 de 22 de agosto, nueva ley de combate o terrorismo. Recuperado de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=119&tabela=leis&so_miolo=

NACIONES UNIDAS. (2018). Actividades de lucha contra el terrorismo, instrumentos jurídicos internacionales. (Recuperado de: http://www.un.org/es/counterterrorism/legal-instruments.shtml

_____. (2014). Protocolo de Montreal. Protocolo que modifica el convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves. pp. 1-2. Recuperado de: http://www.icao.int/secretariat/legal/list%20of%20parties/montreal_prot_2014_es.pdf

_____. (2010a). Convenio de Beijing. Conjunto de textos administrativos para la ratificación del convenio para la represión de actos ilícitos contra la seguridad de la aviación internacional, pp. 1-5. Recuperado de: http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_ES.pdf

_____. (2010b). Protocolo de Beijing, Conjunto de textos administrativos para la ratificación del protocolo complementario del convenio para la represión del apoderamiento ilícito de aeronaves. Doc 9959 pp. 1-4. Recuperado de: http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_protocol_ES.pdf

_____. (2010c). Convenio sobre la marcación de explosivos plásticos para los fines de detección, pp. 1-8. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv10-spanish.pdf

_____. (1999). Convenio internacional para la represión de la financiación del terrorismo, pp. 1-19. Recuperado de: https://treaties.un.org/doc/db/Terrorism/spanish-18-11.pdf

_____. (1998). Convenio internacional para la represión de los atentados terroristas cometidos con bombas, pp. 1-14. Recuperado de: https://treaties.un.org/doc/db/Terrorism/spanish-18-9.pdf

_____. (1992a). Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima, pp. 262-274. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv8-spanish.pdf

_____. (1992b). Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fíjas emplazadas en la plataforma continental, pp. 323-329. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv9-spanish.pdf

_____. (1990). Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, pp. 488-491. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv7-spanish.pdf

_____. (1987). Convención sobre la protección física de los materiales nucleares. pp. 152-160. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv6-spanish.pdf

_____. (1983). Convención internacional contra la toma de rehenes, pp. 238-243. Recuperado de: https://treaties.un.org/doc/db/Terrorism/spanish-18-5.pdf

_____. (1977). Convención sobre la prevención y el castigo de delitos contra personas internacionalmente protegidas, inclusive agentes diplomáticos, pp. 191-195, Recuperado de: https://treaties.un.org/doc/db/Terrorism/spanish-18-7.pdf

_____. (1975). Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, pp. 198-202. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv3-spanish.pdf

_____. (1973). Convenio para la represión del apoderamiento ilícito de aeronaves, pp. 123-127. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv2-spanish.pdf

_____. (1969). Convenio sobre los infractores y ciertos otros actos cometidos a bordo de las aeronaves, pp. 242-251. Recuperado de: https://treaties.un.org/doc/db/Terrorism/Conv1-spanish.pdf

_____. (1945). Carta de las Naciones Unidas. Recuperado de: http://www.un.org/es/sections/un-charter/chapter-i/index.html

NOTICIAS INTERNACIONALES. (13 de diciembre de 2015). Estado Islámico extiende sus tentáculos de captación y entrenamiento a Latinoamérica. *lainformacion.com.* Recuperado de: http://www.lainformacion.com/mundo/estado-islamico-extiende-sus-tentaculos-de-captacion-y-entrenamiento-a-latinoamerica_iR7KLTuwFzmQKffCsdPsc5/

OROYFINANZAS.COM. (29 de abril de 2015). ¿Qué es el SEPBLAC? Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias de España.

OSCE. (2016). Ver su Web: http://www.osce.org/es/whatistheosce/factsheet

OTAN. (2018). North Atlantic treaty organization. Organización del Tratado del Atlántico Norte. Vid. http://www.nato.int/

_____. (7 de marzo de 2017). Cooperative Cyber Defence Centre of Excelence. Cyber Security Documents. Recuperado de: https://ccdcoe.org/cyber-security-strategy-documents.html

_____. (2017). Tallinn Manual Process. NATO Cooperative Cyber Defense Centre of Excellense. Vid. https://ccdcoe.org/tallinn-manual.html

_____. (18 de noviembre de 2015). Recuperado de: http://www.nato.int/cps/en/natolive/news_124868.htm?selectedLocale=en

PARLAMENTO EUROPEO. (2001). Acta del 5 de septiembre de 2001.

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (5 DE JUNIO 2015). DOUE» núm. 141, páginas 73 a 117, Referencia: DOUE-L-2015-81123. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2015-81123

PERIÓDICO DIGITAL, LA INFORMACIÓN. (12 de mayo de 2017) España ha resuelto más de 50.000 ciberataques en lo que va de año, 247 críticos. Recuperado de https://www.lainformacion.com/espana/Espana-resuelto-ciberataques-operadores-estrategicos_0_1025597841.html

POLICIA NACIONAL. Brigada de Investigación Tecnológica de la Policía Nacional (BIT). Recuperado de: https://www.policia.es/org_central/judicial/udef/bit_alertas.html

PRESS DIGITAL. (25 enero de 2016). Europol alerta de que los terroristas del Estado Islámico pueden volver a atentar en Europa. Recuperado de: https://www.pressdigital.es/texto-diario/mostrar/398663/europol-alerta-terroristas-estado-islamico-pueden-volver-atentar-europa

PRESIDENCIA DEL GOBIERNO, ESPAÑA. (1 de diciembre de 2017). Real Decreto 1008/2017, por el que se aprueba la Estrategia de Seguridad Nacional 2017. Un proyecto compartido de todos y para todos Recuperado de http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

_____. (30 de junio de 2011). *Estrategia Española de Seguridad. Una responsabilidad de todos (EES).* Aprobada por el Consejo de Ministros del 24 de junio de 2011. Recuperado de http://www.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf

PWC. (2018). Recuperado de: https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html

REAL INSTITUTO ELCANO. (Julio 2016). THIBER, The Cyber Security Think Tank.*RIE de Estudios Internacionales y Estratégicos* nº 16, Recuperado de: http://www.realinstitutoelcano.org/wps/wcm/connect/dc10afa8-a732-4b8d-a179-be83792d73a5/Ciber_Elcano_Num16.pdf?MOD=AJPERES&cacheid=1468939900564

_____. (Enero 2016). Percepción social del terrorismo yihadista en España. Fernando Reinares. Comentario Elcano 2/2016-25/1/2016,*Estudios Internacionales y Estratégicos*, Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/comentario-reinares-percepcion-social-terrorismo-yihadista-espana

SEPBLAC. (2017). Servicio ejecutivo, comisión de prevención del blanqueo de capitales e infracciones monetarias. Recuperado de: http://www.sepblac.es/espanol/presidencia_gafi/presidencia.htm

SERVICIO DE ABOGADOS. (26 de abril de 2015). Las resoluciones manifestadas: La conspiración, la proposición, la provocación y la apología. Recuperado de:

http://juiciopenal.com/delitos/las-resoluciones-manifestadas-la-conspiracion-la-proposicion-la-provocacion-y-la-apologia/

SUBSECRETARÍA DE DEFENSA, CHILE. (27 de abril de 2017). Una Política de Ciberseguridad para Chile. Recuperado de: http://www.ssdefensa.cl/n5427_27-04-2017.html

THE WHITE HOUSE. Office of the Press Secretary. (2016). The US will invest 19 billion dollars in cybersecurity in 2017 alone, a 35 % increase compared to 2016. 'Fact Sheet: Cybersecurity National Action Plan', 9 February 2016.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, UIT. (2018). Encuesta sobre ciberseguridad año 2016. Recuperado de: https://www.itu.int/itunews/manager/display.asp?lang=es&year=2006&issue=05&ipage=ITU-survey&ext=html

_____. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. Ref. UIT-T X. 1205. Recuperado de: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

XNET, BLOC (2016). Directiva contra el Terrorismo: El Parlamento Europeo contra nuestras libertades. España. Recuperado de: https://xnet-x.net/directiva-terrorismo-recorte-libertades/

BIBLIOGRAFÍA

LEGISLACIÓN DE INTERÉS

Constitución Española, 29 de diciembre de 1978. Boletín Oficial del Estado (BOE) num 311,1. pp. 29315-29339. Recuperado de: https://www.boe.es/boe/dias/1978/12/29/pdfs/A29313-29424.pdf

Instrumento de ratificación del Convenio sobre Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado (BOE). Núm. 226. Sec. I. pp. 78847-78896. Recuperado de: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

Instrumento de ratificación del Tratado de la Unión Europea, 13 de enero de 1994. Firmado en Maastricht el 7 de febrero de 1992. *Boletín Oficial del Estado (BOE)* num. 11. Pp. 858-926. Recuperado de: https://www.boe.es/boe/dias/1994/01/13/pdfs/A00858-00926.pdf

Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado. BOE* núm. 103. Ultima modificación 10 de diciembre de 2013. Versión consolidada. Recuperado de: http://www.prevencionblanqueo.com/wp-content/uploads/2014/04/BOE-Ley-10-10.pdf

Ley Orgánica 13/2015 de 5 de octubre de modificación LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado (BOE)* núm. 239, pp. 90192-90219. Recuperado de: https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP. Cuadro comparativo, observatorio de la justicia y de los abogados, área procesal penal, ilustre colegio de abogados de Madrid, 2015, Recuperado de:

http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, en materia de delitos de terrorismo, (31/03/1995). Boletín Oficial del Estado (BOE) núm. 77.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP

Ley Orgánica 32/2003 de 3 de Noviembre, General de Comunicaciones. *Boletín Oficial del Estado (BOE)*, num. 264. BOE_A-2003-20253. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2003-20253

Ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y de la finmanciación del terrorismo. *Boletín Oficial del Estado (BOE)* nº 103, pp. 37458-37499. 29 de abril de 2010. Recuperado de: https://www.boe.es/boe/dias/2010/04/29/pdfs/BOE-A-2010-6737.pdf

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Jefatura del Estado *Boletín Oficial del Estado (BOE)* núm. 157, de 2 de julio de 1985. Referencia: *BOE*-A-1985-12666. Consolidada 28 de octubre de 2015. Recuperado de: https://www.boe.es/buscar/pdf/1985/BOE-A-1985-12666-consolidado.pdfLey Orgánica 34/2002 de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico. Boletín Oficial del Estado (BOE), num. 166. BOE_A-2002-13758. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *Boletín Oficial del Estado (BOE)*, num. 166. BOE_A-2002-13758. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de carácter personal. *Boletín Oficial del Estado (BOE)*, num. 298. pp. 43088-43099. Recuperado de: https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

Ley Orgánica 10/1995, de 23 de noviembre, CP. Boletín Oficial del Estado (BOE) 281, 24 de noviembre de 1995. pp. 33987-34058.

Ley 36/2015 de 28 de septiembre, de Seguridad Nacional.*Boletín Oficial del Estado (BOE)*. núm. 233, 29 de septiembre de2015. pp. 87106-87117. Recuperado de: https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad*. Boletín Oficial del Estado (BOE)* núm. 20. 23 de enero de 2018. pp. 9186-8190. Recuperado de: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-799.pdf

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la LECrim (Legislación consolidada. Última modificación 6 de octubre de 2015). https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.*BOE* núm. 17 (19 de enero de 2008). Texto consolidado de 8 de marzo de 2012. Recuperado de: https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdfTribunal Supremo, Sala de lo penal. Sentencia nº 119/2007 de 16 de febrero. Recuperado de: http://www.poderjudicial.es/search/contenidos. Action?action=contentpdf&databasematch=TS&reference=524250&links=&optimize=20070426&publicinterface=true

Tribunal Supremo, Sala de lo penal. Sentencia nº 363/2012 de 9 de mayo. Recuperado de: http://www.poderjudicial.es/search/contenidos. Action?action=contentpdf&databasematch=TS&reference=6386450&links=&optimize=20120529&publicinterface=true

Tribunal Supremo, Sala de lo penal. Sentencia nº 400/2016 de 11 de mayo. Recuperado de: http://www.poderjudicial.es/search/contenidos. Action?action=contentpdf&databasematch=TS&reference=7676158&links=&optimize=20160519&publicinterface=true

Tribunal Supremo, Sala de lo penal. Sentencia nº 503/2008 de 17 de julio. Recuperado de: http://www.poderjudicial.es/search/contenidos. Action?action=contentpdf&databasematch=TS&reference=1458813&links

=&optimize=20081002&publicinterface=true

Tribunal Supremo, Sala de lo penal. Sentencia nº. 693/2016 de 27 de julio. Recuperado de: http://www.poderjudicial.es/search/contenidos.Action?action=contentpdf&databasematch=TS&reference=7746350&links=&optimize=20160729&publicinterface=true

Tribunal Supremo, Sala de lo penal. Sentencia nº. 888/2007 de 25 de octubre. Recuperado de: http://www.poderjudicial.es/search/contenidos.Action?action=contentpdf&databasematch=TS&reference=266351&links=&optimize=20071115&publicinterface=true

GLOSARIO DE TÉRMINOS

A
A QUIBUS. Jueces a quibus o de instancia inferior al Tribunal Supremo.
ACCESO. Cada una de las veces que alguien entra a una página de la Web; los accesos son una buena medida de la popularidad de una página.
AL CALAA. En árabe bastión o fortaleza.
AL FIDAA. Foro yihadista en internet.
AL QAEDA. Grupo terrorista fundamentalista Islamico.
AL SHUMUKH AL ISLAM. Foro yihadista en internet.
AL WALAE WA AL- BARAE RM EN EL ISLAM. Titulo de libro de adoctrinamiento del Islam salafista de titulo Lealtad a Dios y hostilidad para los enemigos de Dios y combatirlos.
ALLAH. Alá, nombre del Dios de los musulmanes.
ALNUSRA. Nueva gloria.
ANA Y MIA, WEBS. Webs que fomentan la anorexia.
ANDALUCIA-CERT. Centro de respuesta a incidentes de ciberseguridad.
ANSAR AL MUJAHIDEEN. Foro yihadista en internet.
ARCHIVO BOT. Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario.
B
BAJAR. Pasar un contenido de algún punto de la Internet al ordenador del usuario.
BIG DATA. O macrodatos es un término que hace referencia a una cantidad de datos tal que supera la capacidad del software convencional para ser capturados, administrados y procesados en un tiempo razonable. El volumen de los datos masivos crece constantemente.
BITCOIN. Es una moneda virtual e intangible
BLINDRADARS. Se trata de una técnica de interferencia electrónica de los radares de las torres de control y de los sistemas de seguimiento de aeronaves.
C
CARNIVORE. (En español, carnívoro) es el nombre de un software usado por el FBI como sistema de cibervigilancia.
CASADO. Término usado en el argot yihadista para anunciar acciones o actos de martirio.
CELULAS YIHADISTAS. Grupos de carácter organizado y armado de soldados de la yihad dispuestos a dar su vida por su causa.
CIBERATAQUE. Ataques realizados en el ciberespacio con o a través de medios cibernéticos.
CIBERBULLING. Acoso virtual, atacar a una persona a través de internet.

CIBER-CAFÉ.En el argot yihadista son las salas de Chat para buscar a jóvenes que muestran una predisposición hacia el islamismo radical.
CIBERESPACIO. Entorno virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes, por donde circulan los datos electrónicos de los ordenadores del mundo.
CIBERESPIONAJE. Espionaje tanto personal, comercial o militarrealizado en el ciberespacio con o a través de medios cibernéticos.
CIBER-COALLITION. Ciber ejercicio anual que viene realizando la OTAN donde participa la UE.
CIBERCRIMEN. Crímenes realizados en el ciberespacio con o a través de medios cibernéticos.
CIBERDELINCUENTE. Toda aquella persona que comete un delito en un nuevo ámbito delictivo llamado ciberespacio.
CIBERDELITO. Todos y cada uno de los delitos cometidos en el ciberespacio con o a través de medios cibernéticos.
CIBERPLANNING. Plan de actuación a través del ciberespacio.
CIBERPOLICIA. Policía especializada en actuar en el espacio cibernético sobre delitos cibernéticos.
CIBERSEGURIDAD. El objetivo es garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.
CIBERTERRORISMO.Terrorismo apoyado cibernéticamente es decir cualquier acto terrorista cometido en el ciberespacio con o a través de medios cibernéticos.
COMISION ROGATORIA. Encargo de práctica de diligencia judicial realizado a otro país
CRACKERING. Intrusiones destructivas en sistemas informaticos.
D
DATOS. Representación de información bajo una forma convencional destinados a facilitar su tratamiento.
E
ECHELON. Es la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia
E-MAIL (ELECTRONIC MAIL). Los usuarios de e-mail (correo electrónico) - un equipo basado en la forma de enviar y recibir mensajes a través de Internet. Podrá tener su propia cuenta de correo electrónico o utilizar una cuenta compartida, que es bastante común en el mundo en desarrollo.
ERA DE LA INFORMACION. La etapa actual de desarrollo de la sociedad que comenzó a surgir a finales del siglo XX. Este período se caracteriza por el aumento de la producción, la transmisión, el consumo y dependencia de la información. Muchos consideran que el nuevo papel de la información debe cambiar nuestro comportamiento social y económico de forma tan dramática como lo hizo la Revolución Industrial.
ERROR FACTI. O error inexistente.
F
FACEBOOK. Red social de amigos personales.
FACTUM. Hechos probados.
FATWA. Decreto islámico.
FAVOR LIBERTATIS. Principio de libertad de expresión.
FIN TECH. Su origen es la contracción de las palabras inglesas 'finance' y 'technology', las cuales engloban a los servicios de las empresas del sector financiero las cuales utilizan las nuevas tecnologías para crear productos financieros innovadores.

FLUJO DE DATOS. Transferencia de datos entre constantes, variables o archivos resaltados de la ejecución de instrucciones, procedimientos, módulos de programa o programas.
FORKANE. Grupo guerrillero “forkane”, que, desde una posición defensora del fundamentalismo islámico, luchó en las montañas de la provincia argelina del Chelf en contra del GIA y del ejército argelino, integrados dentro de la organizaciónD.H.D.S.
FRAUDE INFORMÁTICO. Acto mediante el cual una persona engañando a otra o aprovechándose del error en que se halla, obtiene ilícitamente una cosa o lucro individuo, a través de los medios electrónicos.
G
GROOMING / CHILD GROOMING. Acoso sexual a menores.
GOOGLE. Buscador general de información líder en internet, mundialmente conocido.
H
HABEAS DATA. Es una acción jurisdiccional, normalmente constitucional, que puede ejercer cualquier persona física o jurídica, que estuviera incluida en un registro o banco de datos de todo tipo, ya sea en instituciones públicas o privadas, en registros informáticos o no, a fin de que le sea suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada.
HACKEAR. La entrada o acceso a sistemas informáticos con malas ideas de cometer un delito.
HACKING. Tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje.
HARDWARE. Soporte físico; conjunto de elementos físicos empleados para el tratamiento de datos.
HAWKING POLÍTICO. Ciberataque que consiste en denegación de servicio entre países (ejemplo: China-Japón, Árabes-Israelies, India- Pakistán).
I
IMÁN. Jefe religioso musulmán encargado de una jurisdicción.
INFORMACIÓN. Elemento de conocimiento susceptible de ser representado con ayuda de convenciones para ser conservado, tratado o comunicado.
INFORMÁTICA. Ciencia del tratamiento racional, en particular por máquinas automáticas, de la información considerada como el soporte de conocimientos humanos y de comunicaciones en los aspectos técnico, económico y social. Conjunto de disciplinas científicas y de técnicas específicamente aplicables al tratamiento de datos efectuado por medios automáticos.
INMOLARSE. Acción de suicidio en acto de guerra con uso de armas o explosivos destinados a ésta para hacer daño al enemigo.
INTERFACE. Conjunción entre dos soportes físicos o lógicos que les permite intercambiar informaciones mediante la adopción de reglas comunes, físicas o lógicas.
INTERNATIONAL INSTITUTE OF HUMANITARIAN LAWS. Instituto internacional de leyes humanitarias.
J
JABHAT AL NUSRAH. «Frente de la Victoria para el Pueblo de Gran Siria»es una organización terrorista asociada a Al Qaeda que opera en Siria y Líbano.

K
KATIVA. Grupo militar conocido por las fuerzas de seguridad españolas al ser una brigada que integraba a ceutíes en sus filas.
KEYLOGGERS. El envío o instalación de archivos espías en algún hardware de propietario ajeno.
KINETIC OPERATIONS. Entiéndase como aquellas medidas militares que implique la fuerza letal, básicamente tácticas de guerra.
L
LAN (Local Área Network). Un grupo de computadoras conectadas a uno o más servidores comunes para el intercambio de archivos, servicios de impresión y acceso a Internet. Generalmente se encuentran en oficinas y escuelas.
LAS REDES DE CABLE (cable networks). Los sistemas de comunicaciones mediante cable coaxial para la entrega de información. Las redes de cable comenzaron como un medio para la entrega de la programación de televisión, aunque muchas compañías de cable ofrecen servicios de alta velocidad de datos (por ejemplo, Internet) y telefonía a través de sus redes.
M
MALWARE. (Del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado.Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.
MEDIOS CIBERNÉTICOS. Todos aquellos medios tanto físicos como de aprendizaje necesarios para moverse y desenvolverse en el ciberespacio.
MONEDA VIRTUAL: Moneda electrónica sin formato físico utilizada para transacciones cibernéticas.
MUYAHEDINES. Luchadores por la guerra santa, dispuestos a inmolarse por la yihad.
N
NICKNAME. En informática, nickname o nick es un nombre de fantasía o un nombre para abreviar un nombre mayor. La traducción más directa sería apodo o alias.
NOMBRE DE DOMINIO. Una cadena de palabras usadas para identificar direcciones de computadoras en Internet. Comúnmente los puntos al nivel superior de un sitio World Wide Web en un equipo anfitrión.
O
OUSSAMMA. Imán de los Imanes.
P
PACTUM SCALERIS. O concierto previo.
PALTALK. Programa informático de mensajería instantánea.
PASSWORD. Es una combinación de letras y/o números que brinda, a quien lo conoce, la posibilidad de acceder a un recurso. El password sirve como protección y como mecanismo de seguridad.
PETYA. Es un malware de tipo ransomware reportado por la empresa Heise Security, se transmite como troyano usando el popular sistema de archivos.
PHISING. Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo.
PHREAKERS. Es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.

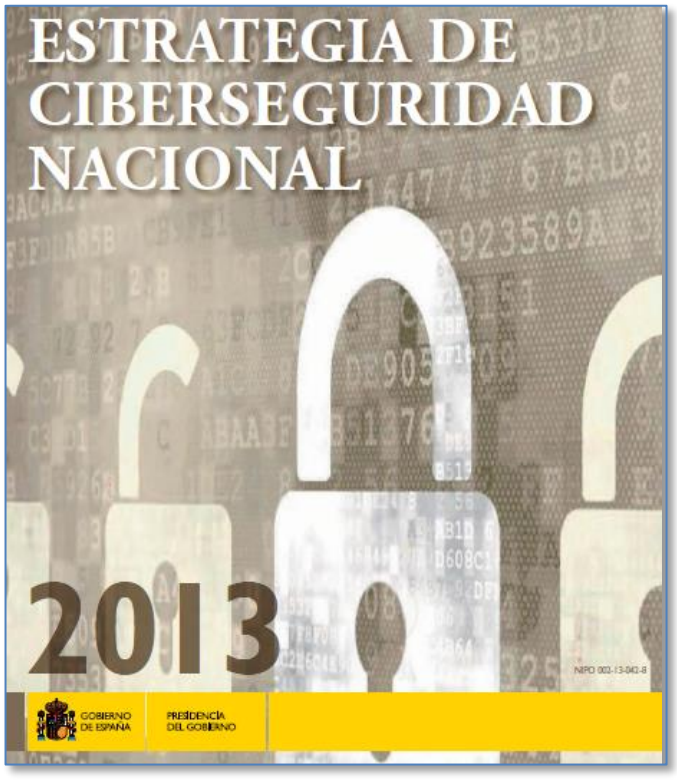
POST. Mensaje o artículo, generalmente usado en el contexto de foros y blogs en Internet
R
RANSOMWARE: (Del inglés ransom, 'rescate', y ware, por software) Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos.
RATIO DECIDENDI. Es la base de donde sacamos la razón de la decisión.
RED DE DATOS. Conjunto de vías de datos, de circuitos de datos y de medios de conmutación que permiten interconectar terminales de datos.
RED MAHDALI- AL LAL. Red creada por dirigentes yihadistas que organizaba el tráfico de combatientes islámicos, capital e información de residentes en España con coordinación de los integrantes marroquíes y ceutíes y de los miembros de la Kativa.
ROOTKITS. Es un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático.
S
SALAFISTA. Doctrina salafista, El salafismo es un movimiento político-religioso fundamentalistasunnita que reivindica el retorno a los orígenes del Islam como base para extender la ideología de extrema derecha del wahabismo saudí y catarí entre los musulmanes
SEDES VIRTUALES. Espacios virtuales en internet que se utilizan para alojar alguna información de carácter promocinal o con idea de reclutar adeptos o financiación.
SERVIDOR. Elemento conectado a un sistema informático que permite la consulta directa de uno o varios bancos de información.
SHABAKA AL HAQIQA AL LKHBARIA. Pagina web denominada verdad informativa.
SHAHID. Mártir.
SHARIA. Ley islámica.
SHEIKS. Sabios musulmanes de influencia que respaldan religiosamente acciones terroristas y que ofrecen implícitamente “un pasaporte al paraíso de los mártires”.
SHURA. Es una palabra árabe que significa “consultar”.
SKETCH. Pequeño espacio o boceto de humor emitido en un medio publicitario.
SMART DEFENCE. Iniciativa que supone que los aliados cooperen entre sí para generar, de forma efectiva y económicamente rentable, las modernas capacidades de defensa que la Alianza requiere.
SNIFFER. Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.
SNUFF. Acciones vinculadas a redes pedófilas y a ritos satánicos o heréticos.
SOFTWARE. Los programas o “instrucciones” que un ordenador necesita para realizar tareas específicas. Ejemplos de software incluyen procesadores de texto, clientes de correo electrónico, navegadores web, juegos de vídeo, hojas de cálculo, herramientas de contabilidad y sistemas operativos.
SPAM. El envío masivo de correo no deseado.
SPOOFING. La suplantación de remitentes de mensajes informáticos.
T
TECHNICAL ARRAGEMENT ON CIBER DEFENCE.El refuerzo en la cooperación entre la OTAN y la Unión Europea (UE) en materia de ciberseguridad se materializó en febrero de 2016 con este Tratado, que permite el intercambio de información entre los equipos de respuesta rápida.

TELECOMUNICACION. Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de toda naturaleza, por cable óptico, radioeléctricos u otros sistemas electromagnéticos.
TELEINFORMÁTICA. Explotación automatizada de sistemas informáticos que utilizan redes de comunicación.
TELEMÁTICA. Conjunto de servicios de naturaleza y origen informáticos que pueden ser provistos a través de una red de telecomunicaciones. Conjunto de servicios diferentes a los servicios telegráficos y telefónicos usuales, que pueden ser obtenidos por los usuarios de una red de telecomunicaciones el cual permite enviar o recibir informaciones o efectuar operaciones particulares, como consulta de archivos, reservaciones u otras transacciones comerciales o bancarias. Ejemplo: Teletex y Videografía.
TROYANOS. Los Troyanos Informáticos o Caballos de Troya son una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos habituales (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño.
TWITTER. Red social de intercambio de mensajes cortos.
U
UKUSA. Sociedad dirigida por países anglosajones (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) que dirige la red de espionaje ECHELON.
UN ANCHO DE BANDA. La cantidad de datos que pueden pasar a través de un determinado canal de comunicaciones en una cantidad estándar de tiempo (generalmente por segundo).
V
VICIOS “IN IUDICANDO”. Vicios inexistentes, proceso con ausencia de vicios.
VIRUS INFORMÁTICOS. Son esencialmente programas de carácter malicioso, que pretenden infectar archivos contenidos en el sistema, con el objeto de producir modificaciones o daños en el sistema informático que han infectado.
W
WANNACRY. También conocido como *WanaCrypt0r 2.0*, es un programa dañino de tipo ransomware.
WEB 2.0. Web social y los medios de comunicación que ofrece también han incorporado este adjetivo, denominándose Medios Sociales o Social Media (...). El cambio se da verdaderamente a nivel usuario, que pasa de ser consumidor de la Web a interactuar con ella y con el resto de usuarios de múltiples formas.
Y
YIHAD. Guerra santa de los musulmanes.
YIHADISTA. Perteneciente o relativo a la yihad o a los yihadistas. Ideología yihadista.
YOUTUBE. Red social de intercambio de videos.

ANEXO I

ESTRATEGIA DE

CIBERSEGURIDAD NACIONAL



www.dsn.gob.es/es/file/146/download?token=Kl839vHG

Capítulo 1
El ciberespacio y su seguridad

El desarrollo de las Tecnologías de Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. El ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas.

El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales de la Política de Ciberseguridad Nacional.

"El desarrollo de las TIC ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo"

Los ataques derivados de estas amenazas, denominados ciberataques, comparten generalmente una serie de características que les son comunes:

Características de los ciberataques

Bajo Coste

- muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido.

Ubicuidad y fácil ejecución

- la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.

Efectividad e impacto

- si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado.

Reducido riesgo para el atacante

- la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción.

La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las Administraciones Públicas, las Infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional.

"La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico"

La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Informa-

ción y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de España depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

Riesgos y Amenazas a la Ciberseguridad Nacional

Capítulo 2
Propósito y principios rectores de la ciberseguridad en España

España precisa de Sistemas de Información y Telecomunicaciones seguros y confiables, tanto en su infraestructura física (equipos y redes), como en su vertiente inmaterial (programas informáticos, modelos o procedimientos). Estos sistemas, al tiempo que posibilitan el acceso de los ciudadanos y empresas al ciberespacio, albergan información valiosa y sustentan servicios estratégicos para nuestra nación, esenciales para el correcto funcionamiento de nuestra sociedad.

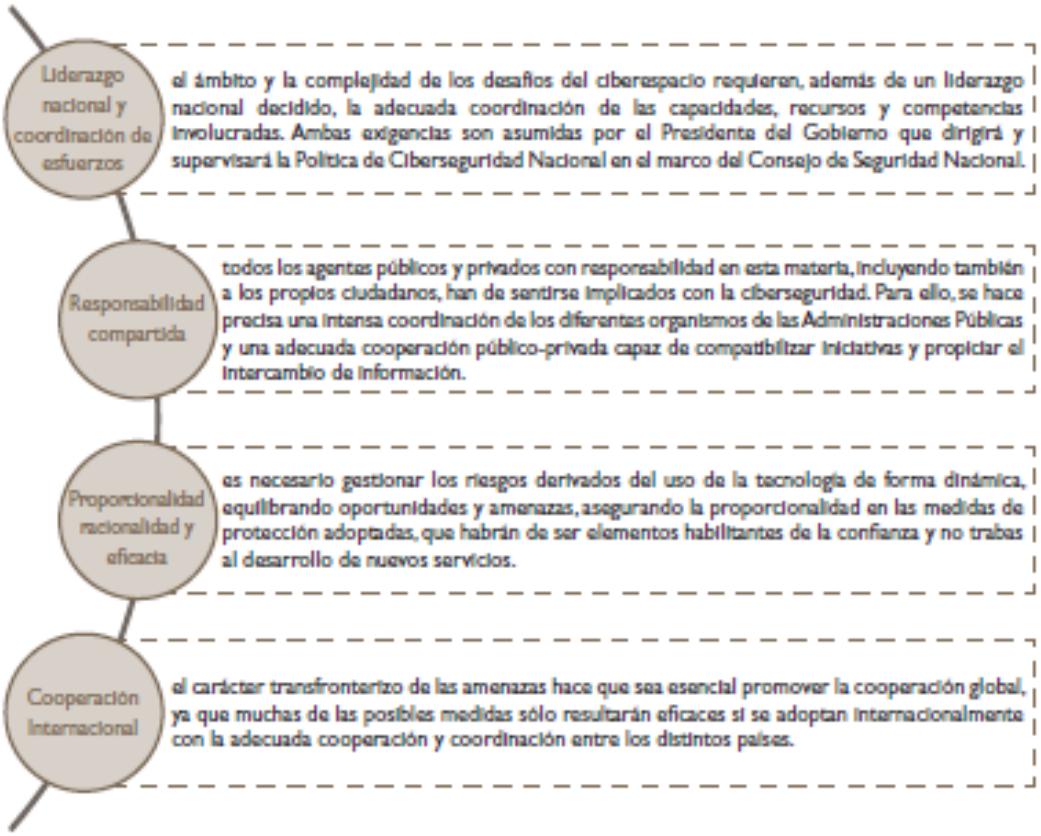
El propósito de la **Estrategia de Ciberseguridad Nacional**, promovida por el **Consejo de Seguridad Nacional** es fijar las directrices generales del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a nuestra nación su seguridad y progreso, a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos. Todo ello dentro del máximo respeto a los principios recogidos en la Constitución; en las disposiciones de la Carta de Naciones Unidas, relativas al mantenimiento de la paz y seguridad internacional; en coherencia con la Estrategia de Seguridad Nacional y con iniciativas desarrolladas en el marco europeo, internacional y regional.

"El propósito de la Estrategia de Ciberseguridad Nacional, promovida por el Consejo de Seguridad Nacional es fijar las directrices del uso seguro del ciberespacio"

Igualmente, alienta la presencia de España en los organismos y foros de carácter internacional canalizando las iniciativas y los esfuerzos internacionales en defensa del ciberespacio.

Principios Rectores

La **Estrategia de Ciberseguridad Nacional**, en sintonía con los principios informadores de la Estrategia de Seguridad Nacional, y como extensión de éstos, se sustenta e inspira en los siguientes Principios Rectores:



Y todos ellos, respetando y fortaleciendo la protección y el pleno disfrute de los derechos fundamentales consagrados en nuestra Constitución y en instrumentos internacionales de la importancia de la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos o el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales. El Gobierno de España se compromete a desarrollar políticas que, mejorando la seguridad de los Sistemas de Información y Telecomunicaciones que emplean los ciudadanos, profesionales y empresas, preserven los derechos fundamentales de todos ellos, especialmente en los sectores más desprotegidos.

Capítulo 3
Objetivos de la ciberseguridad

OBJETIVO GLOBAL

Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.

Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia. Esta Estructura se articulará bajo el principio de eficiencia y sostenibilidad en el uso de los recursos, garantizando unas óptimas capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta de los Sistemas de Información y Telecomunicaciones ante posibles ciberataques.

"Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia"

El fortalecimiento de la ciberseguridad proporcionará a las Administraciones Públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general, una mayor **confianza** en el uso de las TIC. Para ello, los organismos públicos responsables trabajarán en coordinación con el sector privado y con los propios ciudadanos, para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información.

Asimismo, en defensa del interés nacional, la Política de Ciberseguridad Nacional estará alineada con iniciativas similares a las de los países de nuestro entorno, así como con las organizaciones europeas e internacionales competentes, en particular, con la Estrategia de Ciberseguridad de la Unión Europea.

Finalmente, de cara a garantizar la protección de los sistemas y la resiliencia de los servicios de las Administraciones Públicas y las Infraestructuras Críticas, así como la disponibilidad de productos confiables, será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC.

En este sentido, España, manteniendo su política de diversificación y neutralidad tecnológica, velará por la utilización de componentes que estén certificados conforme a normas internacionalmente reconocidas.

Las consideraciones hechas en este objetivo global se aplicarán al resto de los objetivos.

OBJETIVO I

Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia

Buena parte de los sistemas TIC de las Administraciones Públicas españolas, la información contenida en ellos y los servicios que prestan, constituyen activos nacionales estratégicos.

Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública, sus sistemas y servicios, así como de las redes que los soportan. Este marco será clave para desarrollar e implantar servicios, cada vez más seguros.

"Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública"

La adaptación de los sistemas de las Administraciones Públicas a esta realidad pasa por implantar servicios de seguridad en las mismas,

mejorando y ejercitando su capacidad de prevención, detección y respuesta ante incidentes, desarrollando nuevas herramientas y manteniendo actualizado el ordenamiento jurídico.

Asimismo, además de mejorar las capacidades de los sistemas militares de Defensa y de inteligencia es necesario reforzar la seguridad de los Sistemas de Información y Comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio.

Las Administraciones Públicas se involucrarán activamente en un proceso de mejora continua respecto de la protección de sus sistemas TIC. Los poderes públicos están obligados a ser ejemplares en la gestión de la ciberseguridad.

OBJETIVO II

Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular

En aplicación del principio de responsabilidad compartida, las Administraciones Públicas deben mantener estrechas relaciones con las empresas que gestionan los Sistemas de Información y Telecomunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y la mutua comprensión del entorno de la ciberseguridad.

"Se debe asegurar la Protección del Patrimonio Tecnológico de España"

En este sentido, merece especial mención las acciones para asegurar la Protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

Es de interés también determinar el impacto que para España puede tener una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales a la sociedad. Puesto que el sector privado posee la titularidad de buena parte de estos sistemas, las medidas que se adopten en materia de ciberseguridad deberán estar alineadas con los requisitos expresados en la normativa reguladora de Protección de Infraestructuras Críticas, para alcanzar un conjunto integrado de medidas de aplicación a los sectores afectados.

OBJETIVO III

Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio

"Es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales"

Las TIC constituyen un medio, un fin o una combinación de ambos, utilizado tanto por las organizaciones terroristas como por las delictivas para lograr sus objetivos. A esto debe unirse la posibilidad, cada vez mayor, de utilizar el ciberespacio como un objetivo en sí mismo para la perpetración de ataques contra servicios esenciales o Infraestructuras Críticas. En ambos casos deben potenciarse los mecanismos de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación en torno a estas formas de criminalidad.

La actuación policial y judicial del Estado en materia de ciberseguridad deberá adecuarse a los patrones de conducta y a las modalidades delictivas de los terroristas y delincuentes en el ciberespacio, cuyos objetivos suelen ser coincidentes con los tradicionales, pero no su metodología.

Para afrontar adecuadamente estas amenazas, que traspasan en muchos casos las fronteras de los Estados, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz.

Igualmente, se hace necesario fomentar la colaboración ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés policial.

El éxito en la lucha contra el terrorismo y la delincuencia en el ciberespacio exige la articulación de los mecanismos necesarios que mejoren las capacidades de las instituciones policiales y los organismos judiciales competentes.

OBJETIVO IV

Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio

El Gobierno de España, reconociendo la importancia de construir y mantener la confianza en los Sistemas de Información y Telecomunicaciones que usan los ciudadanos, profesionales, empresas y organismos del sector público, acometerá las acciones de información y sensibilización necesarias para asegurar que todos conocen los riesgos de operar en el ciberespacio y poseen los conocimientos y el acceso a las herramientas que posibilitan su protección.

"Las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan"

Al mismo tiempo, las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan. Mantener la confianza del consumidor es fundamental para el éxito de la economía digital. Lo mismo cabe decir de las Administraciones Públicas y de sus relaciones con los ciudadanos.

Por tanto, una función esencial es promover una sólida cultura de ciberseguridad, que proporcione a todos los actores la conciencia y la confianza necesarias para maximizar los beneficios de la Sociedad de la Información y reducir al mínimo su exposición a los riesgos del ciberespacio, mediante la adopción de medidas razonables que garanticen la protección de sus datos, así como la conexión segura de sus sistemas y equipos.

La gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.

OBJETIVO V

Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad

Dada la importancia estratégica de la seguridad en el ciberespacio, es absolutamente prioritario disponer del personal cualificado a todos los niveles: órganos de gobierno, directivo, operativo, técnico y judicial.

"Se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva"

Es importante, además, fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones nacionales confiables que permitan proteger adecuadamente los sistemas frente a las diferentes amenazas.

Para alcanzar esta confianza, se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva. Para ello será necesaria una adecuada coordinación del conjunto de agentes implicados en las TIC, facilitando la colaboración entre empresas y organismos públicos de investigación e impulsando proyectos de evaluación y certificación de la seguridad.

La cualificación del personal encargado de la dirección, gestión e implantación de la ciberseguridad se erige en un objetivo fundamental, especialmente en las Administraciones Públicas y las Infraestructuras Estratégicas y Críticas de interés nacional. Además, la utilización de productos con la seguridad verificada constituye un elemento adicional relevante de protección.

OBJETIVO VI

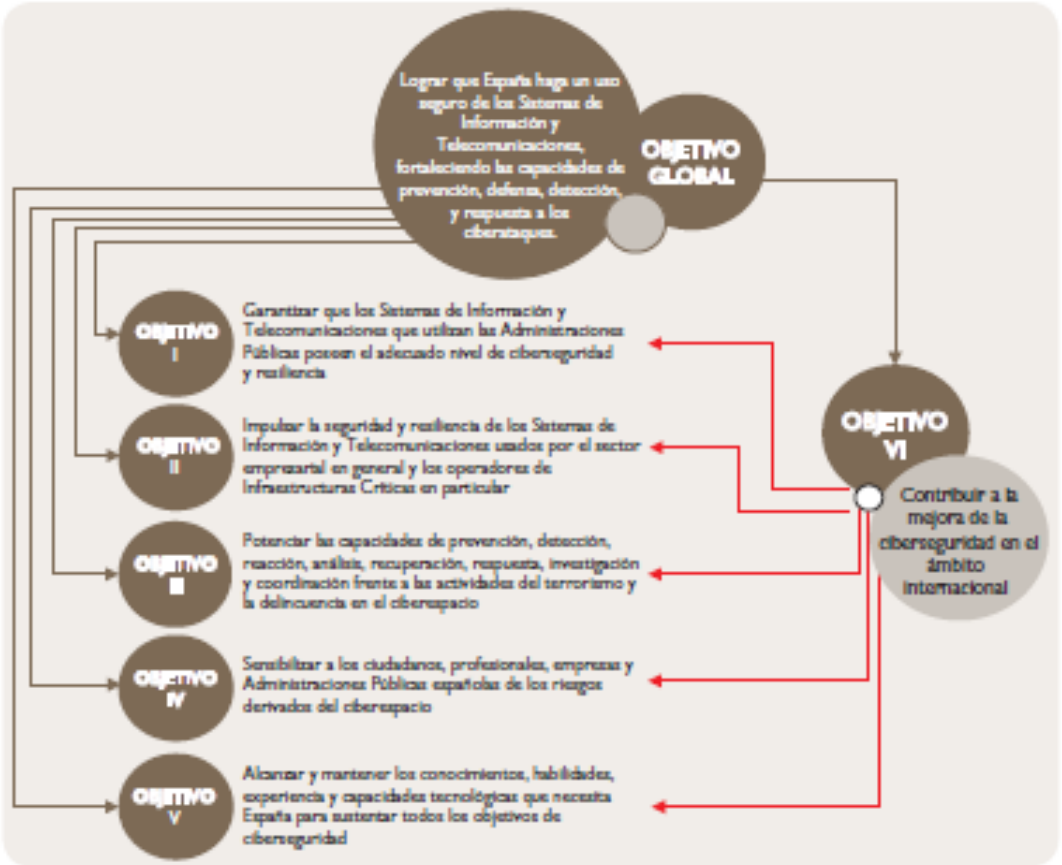
Contribuir a la mejora de la ciberseguridad en el ámbito internacional

Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa en las que participa España, y se colaborará en la capacitación de Estados que lo necesiten, mediante la política de cooperación al desarrollo, ayudándoles a implantar una cultura de la ciberseguridad.

Se fomentará la cooperación en el marco de la UE y con organizaciones internacionales y regionales como, la Agencia Europea de Defensa (EDA), la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el Centro Europeo de Ciberdelincuencia, adscrito a Europol, la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y Desarrollo Económico (OCDE), entre otras.

"Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa"

Junto a los países de nuestro entorno estratégico, se promoverán los esfuerzos dirigidos a conseguir un ciberespacio seguro y fiable, mediante el refuerzo de la colaboración internacional, creando relaciones de confianza para el intercambio de información y datos esenciales en materia de ciberseguridad, y el desarrollo de iniciativas propias de cooperación y desarrollo. Asimismo se llevarán a cabo actuaciones orientadas a impulsar la adopción de estándares internacionales de ciberseguridad y su elevación progresiva.



Capítulo 4: Líneas de acción de la ciberseguridad nacional

Para alcanzar los objetivos señalados, la **Estrategia de Ciberseguridad Nacional** se articula a través de las siguientes Líneas de Acción:

LÍNEA DE ACCIÓN 1

Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas

Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.

En esta línea de acción, el Gobierno de España adoptará las medidas correspondientes, entre ellas:

- Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, y la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales.
- Ampliar y fortalecer las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos de carácter nacional, regional o sectorial, incluyendo a ciudadanos y empresas.
- Garantizar la coordinación, la cooperación y el intercambio de información entre la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales, el sector privado y los organismos competentes de la UE e internacionales para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes.

- Asegurar la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Los CERT de las Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto.

- Desarrollar y mantener actualizadas las instrucciones de prevención y detección, incluyendo procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos ante incidentes de ciberseguridad de ámbito nacional, asegurando su integración en el Sistema de Seguridad Nacional.

- Desarrollar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad, para evaluar y perfeccionar las acciones llevadas a cabo en este ámbito.

- Ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional. Se consolidará la implantación del Mando Conjunto de Ciberdefensa y se potenciará su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés.

- Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

LÍNEA DE ACCIÓN 2

Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas

Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.

Esta línea de acción abarca las iniciativas necesarias para proteger los Sistemas de Información de la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales y sus organismos vinculados o dependientes, así como los Sistemas de Información y Telecomunicaciones e infraestructuras comunes a todas ellas.

Para ello, el Gobierno de España adoptará, entre otras, las siguientes medidas:

- Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados.
- Ampliar y mejorar las capacidades del CERT de las Administraciones Públicas-CCN-CERT- y particularmente de sus Sistemas de Detección y de Alerta Temprana.
- Reforzar las estructuras de seguridad y la capacidad de vigilancia de los Sistemas de Información, en particular los que manejan información clasificada.
- Optimizar el modelo de interconexión de los organismos de las Administraciones Públicas españolas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad.
- Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española (Red SARA), potenciando su uso y sus capacidades de seguridad y resiliencia.
- Desarrollar nuevos servicios horizontales seguros, de acuerdo con directrices de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, organismo responsable de la coordinación, dirección y racionalización del uso de las TIC en la Administración General del Estado.
- Incrementar las actividades nacionales para el desarrollo y evaluación de productos, servicios y sistemas a fin de obtener su certificación apoyando específicamente aquellas que sustenten necesidades de interés nacional.
- Potenciar la creación, difusión y aplicación de las Mejores Prácticas en materia de Ciberseguridad en el ámbito de las Administraciones Públicas.

LÍNEA DE ACCIÓN 3

Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas

Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.

Es necesario incrementar la resiliencia de las Infraestructuras Críticas españolas para evitar una potencial alteración del normal funcionamiento de los servicios esenciales que podrían afectar a la actividad diaria de los españoles.

En este ámbito, el Gobierno de España adoptará, entre otras, las siguientes medidas:

- Asegurar la implantación de la normativa sobre Protección de las Infraestructuras Críticas con el fin de conseguir una seguridad que abarque tanto el ámbito físico como el tecnológico. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan.
- Ampliar y mejorar las capacidades del CERT de Seguridad e Industria, potenciando la colaboración y coordinación con el Centro Nacional para la Protección de Infraestructuras Críticas, con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado.
- Impulsar la participación del sector privado en los Programas de Ejercicios de Simulación de Incidentes de Ciberseguridad.
- Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas.

LÍNEA DE ACCIÓN 4

Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia

Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

Esta línea de acción se concentra en combatir el terrorismo y la delincuencia que actúan en el ciberespacio, en su doble vertiente de instrumento facilitador de sus actividades y de objeto directo de su acción. En este concepto se incluyen también las organizaciones que hacen uso de la tecnología para financiarse o lucrarse, posibilitando la comisión de delitos y el blanqueo de capitales.

En esta línea de acción, el Gobierno de España abordará las medidas correspondientes, entre ellas:

- Integrar en el marco legal español las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes.
- Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados.
- Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana, articulando los instrumentos de intercambio y transmisión de información de interés policial.
- Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

LÍNEA DE ACCIÓN 5

Seguridad y resiliencia de las TIC en el sector privado

Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

Esta línea de acción tiene como objeto la mejora de la seguridad y la resiliencia de las redes, productos y servicios que emplea el sector industrial en el desarrollo de su actividad reforzando la colaboración público-privada con el sector industrial y en particular con el de la seguridad TIC. Se valorará, entre otros, la participación de los Colegios y Asociaciones profesionales.

El Gobierno desarrollará, entre otras, las siguientes medidas:

- Impulsar la cooperación entre los sectores público y privado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional.
- Promover la cooperación con los sectores de la industria y los servicios de la ciberseguridad, con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio, impulsando la participación activa de los proveedores de servicios así como el desarrollo y adopción de códigos de conducta y buenas prácticas.
- Impulsar el desarrollo de estándares en ciberseguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción.

LÍNEA DE ACCIÓN 6

Conocimientos, Competencias e I+D+i

Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.

Esta línea de acción contempla las iniciativas que es necesario acometer para alcanzar y mantener el adecuado nivel de capacitación en ciberseguridad de los profesionales (conocimientos y competencias) e impulsar la industria y la I+D+i españolas. El Gobierno de España procederá a:

- Desarrollar un Marco de Conocimientos de Ciberseguridad en los ámbitos técnico, operativo y jurídico.
- Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especializados.
- Establecer mecanismos que permitan identificar de forma temprana las prioridades y demandas de los poderes públicos en materia de ciberseguridad para su incorporación a las iniciativas anteriores.
- Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación e iniciativas de apoyo a su internacionalización.
- Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades.
- Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional, incluyendo estos criterios en los procesos de desarrollo y adquisición de productos o sistemas.
- Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

LÍNEA DE ACCIÓN 7

Cultura de ciberseguridad

Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

El Gobierno de España, adecuará, potenciará o desarrollará las medidas correspondientes, entre ellas:

- Impulsar las actividades de sensibilización para asegurar que los ciudadanos y empresas tienen acceso a información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico.
- Propiciar el desarrollo de programas de Concienciación en Ciberseguridad, en colaboración con agentes del sector público y privado potenciando, a través de los organismos con competencias en la materia, la necesaria coordinación y racionalización de esfuerzos.
- Fomentar los mecanismos para apoyar a empresas y profesionales en el uso seguro de las TIC, reforzando los conocimientos en materia de seguridad, promoviendo la adopción de herramientas, la difusión de normativa y el uso de buenas prácticas.
- Asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza.

LÍNEA DE ACCIÓN 8

Compromiso Internacional

Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

La globalización tecnológica, sus oportunidades y sus riesgos obligan a alinear las iniciativas de todos los países que persiguen un ciberespacio seguro y confiable. Estos esfuerzos internacionales han de contemplar la elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos.

En esta línea de acción, el Gobierno de España desarrollará, entre otras, las siguientes medidas:

- Potenciar la presencia de España en organizaciones y foros internacionales y regionales sobre ciberseguridad apoyando y participando activamente en las diversas iniciativas y coordinando la posición de los agentes nacionales implicados.
- Promover la armonización legislativa y la cooperación judicial y policial internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo, apoyando la negociación y adopción de convenios internacionales en la materia.
- Propiciar la suscripción de acuerdos en el seno de organizaciones internacionales y con los principales socios y aliados, para fortalecer la cooperación en materia de ciberseguridad y desarrollar un enfoque coordinado de lucha contra las ciberamenazas.
- Impulsar el establecimiento de canales internacionales de información, detección y respuesta.
- Promover la participación coordinada de instituciones públicas y del sector privado en simulacros y ejercicios internacionales.
- En el ámbito de la UE, colaborar en la armonización de legislaciones nacionales, la implantación de la Estrategia de Ciberseguridad de la UE y el impulso de una política internacional en el ciberespacio.
- Fomentar la cooperación con la OTAN en materia de Ciberdefensa, en particular en lo relativo a la respuesta ante incidentes cibernéticos y al intercambio de información técnica sobre amenazas y vulnerabilidades, a la vez que promover dentro de la propia Organización actuaciones que tengan por objeto señalar a la Ciberdefensa como una de sus prioridades.

LÍNEA DE ACCIÓN		CONTENIDO
1	**Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas**	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas**	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas**	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	**Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	**Seguridad y resiliencia de las TIC del sector privado**	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	**Conocimientos, Competencias e I+D+i**	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
7	**Cultura de ciberseguridad**	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	**Compromiso internacional**	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Capítulo 5:
La ciberseguridad en el Sistema de Seguridad Nacional

La visión integral de la ciberseguridad plasmada en esta Estrategia, los riesgos y amenazas detectados que le afectan y los objetivos y líneas de acción trazados, para dar respuesta conjunta y adecuada a la preservación de la ciberseguridad bajo los principios que sustentan el Sistema de Seguridad Nacional, explican la necesidad de contar con una estructura orgánica precisa a estos efectos, que estará constituida por los siguientes componentes bajo la dirección del Presidente del Gobierno:

A. el Consejo de Seguridad Nacional;
B. el Comité Especializado de Ciberseguridad;
C. el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

Estructura orgánica de la ciberseguridad nacional

ESTRUCTURA ORGÁNICA DE LA CIBERSEGURIDAD

a) Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

b) Comité Especializado de Ciberseguridad:

El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad.

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

En el cumplimiento de sus funciones el Comité Especializado de Ciberseguridad será apoyado por el Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

c) Comité Especializado de Situación:

El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno.

"El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno"

El Comité Especializado de Situación será apoyado por el Centro de Situación del Departamento de Seguridad Nacional con el fin de garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Para el cumplimiento eficaz de sus funciones de apoyo al Comité Especializado de Situación, el Centro de Situación del Departamento de Seguridad Nacional podrá ser reforzado por personal especializado proveniente de los departamentos ministeriales u organismos competentes, los cuales conformarán la Célula de Coordinación específica en el ámbito de la Ciberseguridad.

IMPLANTACIÓN

La puesta en marcha del Comité Especializado de Ciberseguridad y del Comité Especializado de Situación, y la armonización de su funcionamiento con los órganos existentes, se realizará paulatinamente mediante la aprobación de las disposiciones normativas necesarias y el reajuste de las vigentes, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes del Sistema de Seguridad Nacional.

ANEXO II

ESTRATEGIA DE CIBERSEGURIDAD INTERNACIONAL. RELACIÓN DE PAÍSES

En este Anexo pueden encontrarse los enlaces de los documentos sobre la política nacional de ciberseguridad de varios países, centrada principalmente en los socios de la OTAN (incluido el Consejo de Asociación Euroatlántico (Euro-Atlantic Partnership Council EAPC), el Diálogo Mediterráneo de la OTAN, la Iniciativa de Cooperación de Estambul (Istanbul Cooperation Initiative ICI) y Socios en todo el mundo). También se incluyen otras estrategias nacionales[327]*.*

[327] OTAN. (7 de marzo de 2017). *Cooperative Cyber Defence Centre of Excelence. Cyber Security Documents. Recuperado de: https://ccdcoe.org/cyber-security-strategy-documents.html*

Naciones de la OTAN:

Albania	
National Security Strategy (2014)	*Original:<http://www.mod.gov.Al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf>*
Cyber Security Strategy (2014)	*Original:<http://www.mod.gov.Al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf>*

Bélgica	
Cyber Security Strategy. Securing Cyberspace (2012)	*Dutch: <https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_nl.pdf* *French: <https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_fr.pdf>*
Cyber Security Strategy for Defence (2014)	*English:<https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf>*

Bulgaria	
White Paper on Defence and the Armed Forces of the Republic of Bulgaria (2010)	*Original:<https://www.mod.bg/bg/doc/drugi/20101130_WP_BG.pdf>* *English:<https://www.mod.bg/en/doc/misc/20101130_WP_EN.pdf>*
Cyber Resilient Bulgaria 2020 (2016)	*English: <https://www.cyberwiser.eu/node/895/pdf>*

Canadá	
Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada (2010)	*English:<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf>*
Action Plan 2010-2015 for Canada's Cyber Security Strategy (2013)	*English:<https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>*
Action Plan for Critical Infrastructures 2014-2017 (2014)	*English:<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf>* *French:<https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-fra.pdf>*

Croacia	
The National Cyber Security Strategy of the Republic of Croatia (2015)	*English:<http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf>*

National legislation. **Information Security Act (2007)**	*English:<http://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Information-Security-Act.pdf>*

República Checa	
Security Strategy of the Czech Republic 2015 (2015)	*Original:<http://www.mzv.cz/file/1386521/Bezpecnostni_strategie_2015.pdf>* *English:<http://www.Army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf>*
White Paper on Defence (2011)	
The Long Term Perspective for Defence 2030 (2015)	*Original:<http://www.mocr.Army.cz/images/id_40001_50000/46088/Dlouhodob___v__hled_pro_obranu_2030.pdf>* *English:<http://www.Army.cz/images/id_8001_9000/8503/THE_LONG_TERM_PERSPECTIVE_FOR_DEFENCE_2030.pdf>*
Cyber Security Strategy of the Czech Republic 2015-2020 (2015)	*English:<https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf>*
Action Plan for the National Cyber Security Strategy 2015-2020	
National legislation. **Act on Cyber Security (2014)**	*English:<https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf>*

Dinamarca	
Danish Defence Agreement 2013-2017 (2012)	*English:<http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf>*
National Strategy for Cyber and Information Security (2014)	*Original:<http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf>*

Estonia	
National Security Concept of Estonia (2010)	*Original<http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/julgeolekupoliitika_alused_2010.pdf>* *English:<http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia_0.pdf>*
National Defence Strategy (2010)	*Original:<http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/riigikaitse_strateegia_2010.pdf>* *English:<http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf>*
Cyber Security Strategy (2014)	*Original:<https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf>*

	English:<https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>

Francia	
White Paper: Defence and National Security (2013)	*Original:<www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf>* *English:<www.defense.gouv.fr/content/download/215253/2394121/file/White%20paper%20on%20defense%20%202013.pdf>*
French National Digital Security Strategy (2015)	*Original:<http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf>* *English:<http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf>*

Alemania	
White Paper 2016 on German Security Policy and the Future of the Bundeswehr (2016)	*Original:<https://www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM0Nzc2YzYyMzcyMDIwMjAyMDIw/Weissbuch2016_barrierefrei.pdf>* *English:<https://www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf>*
Cyber Security Strategy for Germany (2011)	*Original:<http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>* *English:<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>*
National legislation, **IT Security Act (2015)**	*Original:<https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile>* *English:<http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile>*

Hungria	
Hungary's National Security Strategy (2012)	*Original:<http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf>* *English:<http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf>*
Hungary's National Military Strategy (2012)	*Original:<http://www.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf>* *English:<http://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf#!DocumentBrowse>*

National Cyber Security Strategy of Hungary (2013)	
National legislation, **Act on the Electronic Information Security of Central and Local Government Agencies (2013)**	*Original:<http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.240508>*

Islandia	
National Cyber Security Strategy 2015-2026 (2014)	*Original:<https://www.innanrikisraduneyti.is/media/frettir-2014/Netoryggisstefna_drog_11_26---med-frett-a-vefinn.pdf>* *English summary:<https://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf>*

Italia	
White Paper on Defence (2015)	*Original:<http://www.difesa.it/Primo_Piano/Documents/2015/04_Aprile/LB_2015.pdf>* *English:<http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf>*
National Strategic Framework for the Security of Cyberspace (2013)	*Original:<http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf>* *English:<http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>*
National Plan for Cyber Security (2013)	*Original:<http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf>* *English:<http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf>*
Decree on National Cyber Security (2013)	*Original:<http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true>*

Letonia	
The State Defence Concept (2012)	*Original:<http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/Valsts_aizsardzibas_koncepcija_2012. Ashx>* *English:<http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/2012_va_EN. Ashx>*
The National Security Concept (2011)	*Original:<http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/2011_nd. Ashx>* *English:<http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/2011_EN_ND. Ashx>*
Latvian cyber security strategy for the period 2014 to 2018 (2014)	*Original:<https://likumi.lv/doc.php?id=263912>* *English:<https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf>*

***National legislation*,Law on the Security of Information Technologies (2010)**	*English:<http://www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies/>*

Lituania	
National Security Strategy (2017)	*English:<https://kam.lt/download/56659/national%20security%20strategy%202017-01-17.pdf>*
The Military Strategy of the Republic of Lithuania (2016)	*English:<https://kam.lt/download/51934/lt%20military%20strategy%202016.pdf>*
Programme for the Development of Electronic Information Security for 2011–2019 (2011)	*English:<http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf>*
***National legislation*,Cybersecurity Act (2014)**	*Original:<https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf>*

Luxemburgo	
National Strategy on Cyber Security (2011)	*Original:<http://www.gouvernement.lu/3966881/2011-strategie-cybersecurite.pdf>*

Holanda	
National counterterrorism strategy 2011-2015 (2011)	*English:<https://english.nctv.nl/index. Aspx>*
Defence Doctrine (2013)	*Original:<https://www.defensie.nl/>*
International Security Strategy: A Secure Netherlands in a Secure World (2013)	*Original:<www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf>*
National Cyber Security Strategy 2: From Awareness to Capability (2013)	*Original:<www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf>* *English:<https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html>*
Defence Cyber Strategy (2012)	*English:<https://ccdcoe.org/sites/default/files/strategy/NDL-Cyber_StrategyEng.pdf>*

Noruega	
Cyber Security Strategy for Norway (2012)	*English:<https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf>*
Cyber Security Strategy for Norway. Action Plan (2012)	*Original:<https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf>*

Polonia	
National Security Strategy of the Republic of Poland (2014)	*Original:<https://www.bbn.gov.pl/ftp/SBN%20RP.pdf>* *English:<en.bbn.gov.pl/download/3/1314/NSSRP.pdf>*
Cyberspace Protection Policy of the Republic of Poland (2013)	*Original:<www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf>* *English:<www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf>*
Cybersecurity Doctrine of the Republic of Poland (2015)	*Original:<http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf>* *English summary: <http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html>*

Portugal	
National Strategic Defence Concept (2013)	*Original:<http://www.defesa.pt/Documents/20130405_CM_CEDN.pdf>*
National Strategy for the Security in Cyberspace (2013)	*Original:<http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf>*

Rumanía	
Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013)	*Original:<https://www.cert.ro/vezi/document/strategia-de-securitate-cibernetica>*

Eslovaquia	
White Paper on Defence of the Slovak Republic (2016)	*English: <http://www.mosr.sk/white-paper-on-defence-of-the-slovak-republic-2016/>*
Cyber Security Concept of the Slovak Republic for 2015 - 2020 (2015)	*Original:<https://lt.justice.gov.sk/Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645&docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240>* *English:<https://ccdcoe.org/sites/default/files/strategy/SVK_NCSS.pdf>*
Action Plan to the Cyber Security Concept of the Slovak Republic for 2015 - 2020 (2015)	*Original:<https://lt.justice.gov.sk/Attachment/vlastny%20material_rtf.pdf?instEID=-1&attEID=87532&docEID=459073&matEID=8845&langEID=1&tStamp=20151218231602583>*

Eslovenia	
Resolution on the National Security Strategy of the Republic of Slovenia (2010)	*English:<http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/RSNV2010_slo_en.pdf>*
Cyber Security Strategy of the Republic of Slovenia (2016)	*English:<http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf>*

España	
The National Security Strategy: Sharing a Common Project (2013)	*Original:<http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf>* *English:<http://www.lamoncloa.gob.es/documents/estrategiaseguridad_baja_julio.pdf>*
National Cyber Security Strategy (2013)	*Original:<http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>* *English:<http://www.lamoncloa.gob.es/lang/en/Documents/20131332EstrategiadeCiberseguridad_ingl%C3%A9s.pdf>*

Turquía	
2016-2019 National Cyber Security Strategy (2016)	*English:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cybersecurity-strategy-for-turkey/at_download/file>*

Reino Unido	
A Strong Britain in an Age of Uncertainty: The National Security Strategy (2010)	*English:<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf>*
National Cyber Security Strategy 2016-2021 (2016)	*English:<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>*

Estados Unidos de América	
National Security Strategy (2015)	*English:<https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf>*
The National Strategy to Secure Cyberspace (2003)	*English:<https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>*
Cyberspace Policy Review (2009)	*English:<https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf>*
International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (2011)	*English:<https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>*

Draft Strategy for Improving Critical Infrastructure Cybersecurity (2014)	*English:<https://www.nist.gov/>*
President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity (2013)	*English:<https://obamawhitehouse. Archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>*
The Department of Defence Cyber Strategy (2015)	*English:<http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf>*
National legislation, **Cybersecurity Act of 2015**	*English:<https://www.congress.gov/bill/114th-congress/house-bill/2029/text#toc-H7809EA2FFB554972A844FC3D6A472EB8>*
National legislation, Cybersecurity Enhancement Act of 2014	*English:<https://www.congress.gov/bill/113th-congress/senate-bill/1353/text?q=%7b%22search%22:%5b%22cybersecurity%22%5d%7d>*
National legislation, National Cybersecurity Protection Act of 2014	*English:<https://www.congress.gov/bill/113th-congress/senate-bill/2519/text?q=%7b%22search%22:%5b%22cybersecurity%22%5d%7d>*

Naciones no pertenecientes a la OTAN. Europa:

Austria	
Austrian Security Strategy (2013)	*Original:<http://www.bmi.gv. At/cms/BMI_Service/STS/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf>*
National ICT Security Strategy Austria (2012) Original	*English:<https://www.bka.gv. At/>*
Austrian Cyber Security Strategy (2013) Original	*Original:<https://www.bka.gv. At/cyber-sicherheit-egovernment>* *English:<http://www.bmi.gv. At/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf>*

Bosnia yHerzegovina	
Bosnia and Herzegovina Strategy for Prevention and Fight Against Terrorism (2010)	*Original:* *English:<www.msb.gov.ba/dokumenti/BiH%20Strategy%20for%20Prevention%20anf%20Fight%20against%20Terrorism.doc>*

Chipre	
Cybersecurity Strategy of the Republic of Cyprus (2013)	*English:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf>*

Finlandia	
Security Strategy for Society (2010)	
Finnish Security and Defence Policy (2012)	*Original:<http://vnk.fi/documents/10616/622970/J0512_Suomen+turvallisuus-+ja+puolustuspolitiikka+2012.pdf/b534174a-13bc-4684-beb0-a093be30ce2a?version=1.0>* *English:<https://www.bbn.gov.pl/ftp/dok/07/FIN_Finnish_Security_Defence_Policy_2012_Government_Report.pdf>*
Finland's Cyber Security Strategy (2013)	*English:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf>*
Finland's Cyber Security Strategy - Background Dossier (2013)	

Georgia	
National Security Concept of Georgia (2014)	*English:<http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept. Aspx?lang=en-US>*
Cyber Security Strategy of Georgia 2012-2015	*Original:<https://matsne.gov.ge/ka/document/view/1923932>* *English:<http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf>*

Irlanda	
White Paper on Defence (2015)	*Original:<http://www.defence.ie/WebSite.nsf/WP2015Ib>* *English:<http://www.defence.ie/WebSite.nsf/WP2015E>*
National Cyber Security Strategy 2015-2017	*Original:* *English:<http://www.dccae.gov.ie/communications/SiteCollectionDocuments/Internet-Policy/NationalCyberSecurityStrategy20152017.pdf>*

Malta	
Malta Cyber Security Strategy (2016)	*English:<http://mita.gov.mt/en/maltacybersecuritystrategy/Pages/Malta-Cyber-Security-Strategy-2016. Aspx>*

Montenegro	
Strategy on Cyber Security of Montenegro to 2017 (2013)	*English:<www.mid.gov.me/ResourceManager/FileDownload.Aspx?rid=165416&rType=2&file=Cyber%20Security%20Strategy%20for%20Montenegro.pdf>*

Rusia	
National Security Strategy of the Russian Federation (2015)	*Original:<http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf>*
Military Doctrine of the Russian Federation (2014)	*Original:<http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>*
Concept of the Foreign Policy of the Russian Federation (2013)	*Original:<http://www.mid.ru/ru/home>* *English:<http://www.mid.ru/en/main_en>*
National Security Strategy 2009-2020 (2008)	*English:<http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020>*
National Security Concept of the Russian Federation (2000)	*English:<http://www.mid.ru/en/main_en>*
Renewal underway. Information Security Doctrine of the Russian Federation (2016 draft)	*Original:<http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>* *English:*
Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013)	*English:<https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>*
Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011)	*Original:<http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>* *English:<https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf>*

Serbia	
White Paper on Defence of the Republic of Serbia (2010)	*Original:<http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/Bela_Knjiga-Srpski.pdf>* *English:<http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/Bela_Knjiga-Engleski.pdf>*
National legislation, **Cyber Law (draft as of 2015)**	*Original:<http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/zakoni/ZAKON%20O%20VBA%20I%20VOA_CIR.pdf>*

Suecia	
Sweden's Defence Policy 2016 to 2020 (2015)	*Original:<http://www.regeringen.se/contentassets/266e64ec3a254a6087ebe9e413806819/proposition-201415109-forsvarspolitisk-inriktning--sveriges-forsvar-2016-2020>* *English:<http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020>*

Suiza	
National Strategy for Switzerland's Protection Against Cyber Risks (2012)	*Original:<https://www.isb. Admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.download.pdf/Strategie_zum_Schutz_der_Schweiz_vor_Cyber-Risiken_k-DE.pdf>* *English:<https://www.isb. Admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.download.pdf/Strategie_zum_Schutz_der_Schweiz_vor_Cyber-Risiken_k-ENGL.pdf>*

Ucrania	
Draft National Security Strategy (2015)	*Original:<http://www.niss.gov.ua/public/File/2015_analit/strategiya_2015.pdf>*
Cyber Security Strategy (2016)	*Original:<http://www.president.gov.ua/documents/962016-19836>*

Unión Europea	
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013 (2013)	*English:<ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>*

Ásia y Oceanía:

Afganistán	
National Cyber Security Strategy of Afghanistan (NCSA) (2014)	*English:<http://mcit.gov. Af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf>*

Australia	
Strong and Secure. A Strategy for Australia's National Security (2013)	*English:<http://apo.org. Au/files/Resource/dpmc_nationalsecuritystrategy_jan2013.pdf>*
2016 Defence White Paper (2016)	*English:<http://www.defence.gov. Au/WhitePaper/Docs/2016-Defence-White-Paper.pdf>*
Cyber Security Strategy (2009)	*English:https://www. Ag.gov. Au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf*
Cyber Security Strategy. Enabling innovation, growth & prosperity (2016)	*English:<https://cybersecuritystrategy.dpmc.gov. Au/assets/img/PMC-Cyber-Strategy.pdf>*

Azerbaiyan	
National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the years 2014-2020 (2014)	*Original:<http://president. Az/articles/11312>*

Bangladesh	
National Cybersecurity Strategy (2014)	*English:<http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf>*

China	
National Security Strategy (2015)	*Original:http://news.sina.com.cn/c/2015-01-23/180531437149.shtml*
National Military Strategy (2014)	*English:<https://news.usni.org/2015/05/26/document-chinas-military-strategy>*
National Cybersecurity Strategy (2016)	*English:<https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/>*
International Strategy of Cooperation on Cyberspace (2017)	*English:<http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm>*
National legislation **Cybersecurity law of the People´s Republic of China (2016)**	*English:<http://www.chinalawtranslate.com/bilingual-2016-cybersecurity-law/?lang=en>*

India	
National Cyber Security Policy (2013)	*English:<http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf>*

Israel	
Advancing National Cyberspace Capabilities, Government Resolution No. 3611 (2011)	*Original:<http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611. Aspx>* *English:<http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>*
Advancing National Regulation and Governmental Leadership in Cyber Security, Government Resolution No. 2443 (2015)	*English:<https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf>*
Advancing the National Preparedness for Cyber Security, Government Resolution No. 2444 (2015)	*English:<https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf>*

Japón	
Japan Defense (2015)	*Original:<http://www.mod.go.jp/j/publication/wp/wp2015/w2015_00.html>* *English:<http://www.mod.go.jp/e/publ/w_paper/2015.html>*
Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigorous Cyberspace (2013)	*English:<http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>*
International Strategy on Cybersecurity - j-Initiative for Cybersecurity (2013)	*English:<http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf>*
Cyber Security Strategy (2015)	*English:<http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>*

Jordania	
National Information Assurance and Cyber Security Strategy (NIACSS) (2012)	*English:<http://nitc.gov.jo/PDF/NIACSS.pdf>*

Malasia	
The National Cyber-Security Policy (2006)	*English:<nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp>*

Mongolia	
National Security Concept of Mongolia (2010)	*English:<http://www.nsc.gov.mn/sites/default/files/images/National%20Security%20Concept%20of%20Mongolia%20EN.pdf>*
Program on Information Security (2010)	*English:<http://www.crc.gov.mn/en/k/1g/1q>*

Nueva Zelanda	
New Zealand National Security System (2011)	*English:<http://www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf>*
Defence White Paper (2010)	*English:<http://www.nzdf.mil.nz/downloads/pdf/public-docs/2010/defence_white_paper_2010.pdf>*
New Zealand's Cyber Security Strategy (2015)	*English:<http://www.dpmc.govt.nz/dpmc/publications/nzcss>*
New Zealand's Cyber Security Strategy Action Plan (2015)	*English:<http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-action-plan-december-2015.pdf>*
National Plan to Address Cybercrime (2015)	*English:<http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdfZ>*

Pakistán	
National Cyber Security Council Act (2014)	*English:<http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf>*

Qatar	
Qatar National Cyber Security Strategy (2015)	*English:<www.ictqatar.qa/en/cyber-security/national-cyber-security-strategy>*

Samoa	
Samoa National Cyber Security Strategy (2017)	*English:<http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf>*

Arabia Saudita	
National Information Security Strategy in Saudi Arabia (in development as of Feb 2013)	*English:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-of-saudi-arabia/at_download/file>*

Singapur	
National Cyber Security Masterplan 2018 (2013)	*English:<https://www.tech.gov.sg/IDA.html>*
Cyber security strategy (2016)	*English:<https://ccdcoe.org/sites/default/files/documents/SingaporeCybersecurityStrategy.pdf>*

Corea del Sur	
Defense White Paper (2014)	*Original:<http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_20150108030001584O.pdf>* *English:<http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_20150616115616457O.pdf>*
National Cybersecurity Masterplan (2011)	*English:<https://ccdcoe.org/sites/default/files/strategy/KOR_NCSS_2011.pdf>*

Emiratos Arabes Unidos	
National Cyber Security Strategy (2014)	*English:<https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwiWqd7fvqTTAhXGfxoKHeqVAXsQFghKMAQ&url=http%3A%2F%2Fwww.id.gov.Ae%2Fassets%2FkKbkN9NSOGI.pdf.Aspx&usg=AFQjCNFijLycojrr-pveK4zJ-Clquw-sSg&sig2=qIjvdW6D4AD4D3IZtri4UA&bvm=bv.152479541,d.d2s>*

África

Botswana	
National cyber security strategy April 2015	*English:<http://www.cto.int/news/botswana-launches-national-cybersecurity-strategy-project-at-commonwealth-cybersecurity-forum-2015/>*

Egipto	
National ICT Strategy 2012-2017 (2013)	*English:<http://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf>*

Gambia	
National cyber security strategy March 2015	*English:<http://allafrica.com/stories/201512212126.html>*

Ghana	
Ghana National Cyber Security Policy & Strategy (2014)	*English:<http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Ghana_2014_NationalCyberSecurityPolicyStrategyFina.pdf>*

Kenia	
Cybersecurity Strategy (2014)	*Original:<* *English:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/KE_NCSS.pdf>*

Mauritania	
National Strategy for Modernization of Administration and ICT 2012-2016 (2012)	

Mauricio	
National Cyber Security Strategy 2014-2019 (2014)	*English:<http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf>*

Marruecos	
National Strategy for Information Society and Digital Economy 2013	*French:<https://ccdcoe.org/sites/default/files/strategy/Maroc_CyberSecurity_2013_FR.pdf>* *English:<https://ccdcoe.org/sites/default/files/strategy/Maroc_CyberSecurity_2013_ENG.pdf>*

Nigeria	
National Cybersecurity Policy (2014)	*English:<https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf>*
National Cybersecurity Strategy (2015)	*English:<https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf>*

República Sudafricana	
South African Defence Review (2014)	*English:<http://www.gov.za/sites/www.gov.za/files/dfencereview_2014.pdf>*
Cyber Security Policy of South Africa (2010)	*English:<http://pmg-assets.s3-website-eu-west-1.Amazonaws.com/docs/100219cybersecurity.pdf*
National Cybersecurity Policy Framework (2012)	*English:<http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf>*

Tanzania	
National cyber security strategy - drafting underway (June 2016)	

Uganda	
National Information Security Strategy (2011)	*English:<http://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf>*

Zimbaue	
Cyber Security Policy (drafting ongoing as of November 2013)	

Unión Africana	
African Union Convention on Cyber Security and Personal Data Protection (2014)	*English:<https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf>*

América y El Caribe

Brasil	
Defense White Paper	*Original:<http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>* *English:<http://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf>*

Colombia	
National Cybersecurity and Cyberdefense Policy (2011)	*Original:<http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>* *English:<https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf>*
Strategic Innovation Agenda on Cybersecurity(2014)	*Original:<http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf>*

Costa Rica	
National cyber security strategy, **Development announced March 2015**	*Original:<http://www.data.cr/estrategia-de-ciberseguridad-en-costa-rica-plantea-proteger-datos-en-internet/>*

Granada	
National cyber security strategy, **Development announced Feb 2014**	

Jamaica	
Jamaica National Cyber Security Strategy (2015)	*Spanish:<https://www.sites.oas.org/cyber/Documents/Jamaica%20National%20Cyber%20Security%20Strategy%20(Spanish).pdf>* *English:<http://mstem.gov.jm/sites/default/files/Jamaica%20National%20Cyber%20Security%20Strategy.pdf>*

Panamá	
National Strategy for Cyber Security and Critical Infrastructure Protection (2013)	*Spanish:<https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf>*

Trinidad yTobago	
National Cyber Security Strategy (2012)	*Spanish:<https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(Spanish).pdf>*

ANEXO III

Áreas Comunes de Cooperación Estratégica Internacional en ciberseguridad portuguesa

Áreas Comuns de Cooperação Estratégica Internacional no Ciberespaço	Linhas de Desenvolvimento	OTAN	UE
Documentos Estratégicos de Referência		Conceito Estratégico (2010) Política de Ciberdefesa (2011)	Estratégia de Segurança Europeia (2008) Agenda Digital para a Europa (2010-20) Estratégia de Cibersegurança da UE (2013)
Defesa Coletiva	**Cibersegurança/ Ciberdefesa**	Ciberdefesa (área prioritária)	Cibersegurança e Ciberdefesa (áreas prioritárias)
	Combate ao Terrorismo	Combate ao Terrorismo (área prioritária)	Combate ao Cibercrime em geral (área prioritária)
	Proteção de Infraestruturas Críticas	Segurança Energética (área prioritária)	Proteção das Infraestruturas Críticas de Informação (área prioritária)
	Impacto das novas Tecnologias	Análise das Tecnologias Emergentes (área prioritária)	Desenvolvimento de recursos tecnológicos e industriais de cibersegurança (área prioritária)
Gestão de Crises	**Cooperação Civil-Militar**	Aproximação Civil-Militar (*Comprehensive Approach*)	Aproximação Civil-Militar (*Comprehensive Approach*)
	Compreensão do Ambiente Internacional	Monitorização/Análise do Ambiente Internacional	Estabelecimento de uma política internacional coerente do ciberespaço e promoção dos valores-chave da UE (área prioritária)
	Partilha de Informações *(Intelligence Sharing)*	Melhoria da partilha de Informações	Melhoria da partilha de Informações
Segurança Cooperativa	**Segurança e Defesa**	EU e Rússia	OTAN
	Cibersegurança/ Ciberdefesa	UE	OTAN, USA, China e Índia
Desenvolvimento de Capacidades Cooperativas Área da Cibersegurança/ Ciberdefesa		Iniciativas de *Smart Defence* POC:Information Assurance and Cyber Defence Capability Panel (CaP4 IACD)	Iniciativas de *Polling&Sharing* POC: ENISA e Project Team on Cyber Defence (PT CD), da EDA.
	Doutrina e Organização	➢Política, Plano de Ação e Conceito de Ciberdefesa OTAN, como referência. ➢Partilha de informação e melhores práticas.	➢Conceito de Computer Network Operations e Conceito de Ciberdefesa da UE, como referência. ➢Partilha de informação e melhores práticas;
	Interoperabilidade	➢Sinergias civis/militares e cooperação com a comunidade de cibersegurança civil. Ex: NATO Crypto Interoperability Strategy (cooperação OTAN-EU); NATO PKI; NOLCE File Encryption; NATO Common Criteria CaT.	➢Desenvolvimento, na área da cibersegurança, de uma rede europeia de CERTs (Ex:ENISA). ➢Na área da ciberdefesa, exploração de sinergias civis/militares e cooperação com a comunidade de cibersegurança civil.
	Instalações	➢Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa.	➢Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa;
	Liderança e Pessoal	➢Campanhas coordenadas de sensibilização e formação na área da ciberdefesa.	➢Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;
	Material e Tecnologia	➢Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. Ex: Multi National Cyber Defence Capability Development (MNCD2); NATO Information Assurance Product Catalogue (NIAPC); ➢*Pool* de capacidades de ciberdefesa para apoio às operações OTAN.	➢Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. ➢*Pool* de capacidades de ciberdefesa para Quartéis-Generais de nível Operacional e Tático (OHQ/FHQ)
	Treino e Exercícios	➢*Pooling* de recursos de treino/educação; ➢Partilha de informação sobre ameaças e incidentes em contexto operacional de ciberdefesa para apoio de missões OTAN (POC: NCIRC). ➢Exercício NATO Cyber Coalition.	➢*Pooling* de recursos de treino/educação; ➢Partilha de informação sobre ameaças e incidentes em contexto operacional de cibersegurança (POC ENISA) e ciberdefesa (POC EUMS) para apoio de missões de segurança e defesa da UE (missões CSDP). ➢Exercício Cyber Europe.

ONU	OCDE	Relevância Estratégica	Relevância Operacional	Relevância Económica	Área Nova?
Guia para Elaboração da Estratégia Nacional de Cibersegurança (2011) Tratado Internacional das Telecomunicações (2012)	Guidelines Seg SI e Redes (2002) Recomendação Coop Internacional na Lei Proteção Privacidade (2007)	Elevada **= E;** Média = **M**; –Baixa = **B**			**S**-Sim; **N**-Não
Cibersegurança/e-Governance (área prioritária)	Cibersegurança (área estruturante economia global)	**E**	**E**	**E**	**S**
Regulação do Ciberespaço (área prioritária)	Combate ao Cibercrime e Privacidade (área prioritária)	**E**	**E**	**B**	**N**
Contenção de ataques de larga escala (área prioritária)	Proteção SI e Redes (área prioritária)	**E**	**E**	**M**	**S**
e-Governance e normalização (área prioritária)	Monitorização impacto económico das TIC (área prioritária)	**E**	**E**	**E**	**N**
Cooperação política	Cooperação Político-Económica	**E**	**E**	**M**	**S**
Monitorização do ambiente internacional	Monitorização de Mercados e Economia Global	**E**	**E**	**M**	**N**
Troca de informação em *fora* especializados	Troca de informação em *fora* especializados	**E**	**E**	**M**	**N**
Cooperação Internacional	Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	**N**
Cooperação Internacional	Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	**S**
Tratados Internacionais POC: Global Cybersecurity Agenda (GCA), da ITU.	Recomendações e Guidelines POC: Working Party On Information Security And Privacy, da OCDE.	**E**	**E**	**E**	**S**
➢Princípios de regulação e cooperação no ciberespaço. ➢Partilha de informação e melhores práticas	➢Recomendações e orientações. ➢Partilha de informação e melhores práticas	**E**	**E**	**M**	**S**
➢Adoção de políticas, princípios de normalização e requisitos técnicos	➢Adoção de políticas, princípios de normalização e requisitos técnicos	**E**	**E**	**E**	**N**
➢desenvolvimento de centros especializados para cooperação internacional	➢desenvolvimento de centros especializados para cooperação internacional	**E**	**E**	**B**	**N**
Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;	campanhas de sensibilização na área da cibersegurança;	**E**	**E**	**B**	**N**
Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	**E**	**E**	**E**	**S**
➢*Pooling* de recursos de treino/educação existentes;	Nada a referir.	**E**	**E**	**B**	**S**

Ilustración 47: *Áreas de Cooperación Internacional Comunes*[328].

[328] INSTITUTO DE DEFENSA NACIONAL, PORTUGAL. (Diciembre 2013). Ob. Cit., pp. 74-75, Figura 2 - Tabla 1 - Áreas de Cooperación Internacional Comunes.

ANEXO IV

CUADRO COMPARATIVO

ACTUALIZACIÓN LEYES 2015

Cuadro comparativo, Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, CP. Observatorio de la justicia y de los abogados, área procesal penal, Ilustre Colegio de Abogados de Madrid, 2015.

Ver Tabla comparativa en:

http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

ANEXO V

GUÍA ANÁLISIS DE SENTENCIAS

INSTRUMENTO PARA ANALIZAR LAS SENTENCIAS

GUÍA PARA EL ANÁLISIS DE SENTENCIAS	
INVESTIGADOR	
NOMBRE:	
FECHA:	
PROYECTO:	
1. CONTEXTO (ideas claras; frases cortas. Use viñetas)	
1.1.IDENTIFICACIÓN	
NÚMERO:	Se trata de la forma en la que se identifica la sentencia. Inicia con las letras STS. Ejemplo: STS001/2016
FECHA y LOCALIDAD.	Indicar la fecha en la que se adoptó la decisión y donde se realizó.
MAGISTRADO PONENTE:	Se trata del Magistrado que formulo la decisión; quien le propuso a la sala que se tomara esa decisión. Se encuentra habitualmente con la sigla MP. Ejemplo: MP **MANUEL MARCHENA GÓMEZ**.
VOTO PARTICULAR:	Indicar aquí cuál o cuáles magistrados realizaron un voto particular. Los votos particulares se presentan cuando un magistrado se encuentra en desacuerdo con la decisión tomada por la sala. En ese evento, el magistrado debe esgrimir su desacuerdo en un escrito separado que se encuentra al final del documento, después del “Resuelve” aprobado por la mayoría. Los votos particulares pueden ser totales o parciales, dependiendo de si el magistrado se encuentra total o parcialmente en desacuerdo con lo decidido.

1.2. NORMA DEMANDADA (transcripción de los puntos demandados. Si es muy larga, es posible hacer un pequeño recuento acerca de lo que trata y sólo transcribir lo relevante al tema)
Indicar aquí, la norma que fue demandada. De ser posible, transcribir los puntos demandados o hacer un recuento de los que la norma dice.
1.3. PROBLEMA JURÍDICO ENUNCIADO POR EL TRIBUNAL SUPREMO

Indicar aquí cuál es el problema jurídico que el Tribunal enuncia que va a tratar. Si no es muy largo, transcribirlo o copiarlo y pegarlo. El problema jurídico es, por regla general, un enunciado en forma de pregunta que va a guiar la argumentación de la decisión. 1) Normalmente, las sentencias tienen un epígrafe llamado "problema jurídico"; 1.1) algunas veces, se encuentra claramenteel enunciado en forma de pregunta puesto que se encuentra entre signos de interrogación; 1.2) otras veces, en el contenido del epígrafe, no se encuentra una pregunta como tal. En ese caso, habrá que seleccionar solo la parte en la que el Tribunal "se cuestiona"o enuncia qué asuntos debe tratar para poder tomar la decisión. 2) Es bastante inusual encontrar una sentencia sin un problema juridico enunciado por el Tribunal. De ser el caso, indicaremos que no hay.
Ahora bien, en una misma decisión puede haber varios problemas jurídicos enunciados por el Tribunal. En ese caso, seleccionaremos el problema jurídico principal de acuerdo con el tema por el cual analiza la sentencia, sin embargo, es posible también analizar, secundariamente otros problemas jurídicos.

1.4. NORMAS JURÍDICAS RELEVANTES PARA EL CASO

Seleccionaremos las normas constitucionales importantes para la resolución del caso. Éstas pueden encontrarse tanto en la demanda como en la motivación de la decisión. Normalmente, cada una de estas normas determina una argumentación específica.

1.5. DEMANDA (principales argumentos)

En frases cortas y viñetas con cada idea, resumiremos aquí los argumentos queesgrimió el demandante para justificar la inconstitucionalidad de la norma demandada.

1.6. DECISIÓN

Indicaremos aquí cuál es el "resuelve"de la decisión. Si no es muy largo, se transcribe o copiar y pegar; sino, indicar en qué consiste.

2. ARGUMENTO DE LA DECISIÓN (ideasclaras;frasescortas.Usar viñetas)

2.1. PROBLEMA JURÍDICO RESUELTO POR LA SENTENCIA (no necesariamente es el enunciado por ésta)

El **problema jurídico** es una pregunta que revela la confrontación específica de principios jurídicos para la resolución de un caso. Determina el *quid* del asunto. Un importante número de veces, el problema jurídico enunciado por el Tribunal dista de aquel que ella resuelve. Es por esto que el problema jurídico que ella resuelve hay que construirlo. Para ello, aconsejo partir del problema jurídico enunciado por el tribunal e ir depurando a medida que la misma *ratio decidendi* vaya mostrando qué es lo que se pregunta el Tribunal.
En efecto, eventualmente el Tribunal usa problemas jurídicos muy abstractos o generales que no son los problemas jurídicos apropiados. Así por ejemplo ¿Es contrario a la constitución el artículo X de la ley Y? es un problema jurídico trivial. Es decir, obviamente que se busca saber si la norma demandada es inconstitucional –ese es el objeto del control de constitucionalidad concentrado pero no permite saber cuál es la confrontación puntual entre principios o categorías jurídicas. El problema jurídico necesita ser mucho más específico para mostrar la tensión entre la norma demandada y la constitución. Un mejor problema jurídico podría ser ¿Se encuentra justificado un tratamiento desigual favorable para las madres cabeza de familia con relación a los padres cabeza de familia en la asignación de un subsidio para la alimentación de sus hijos? Es posible que en una misma sentencia se traten varios problemas jurídicos, por eso debemos revisar cuál es el problema jurídico principal de la decisión de acuerdo con el tema por el cual se esté analizando la decisión. Sin embargo, de manera secundaria, es posible analizar otros

2.2. RATIO DECIDENDI (rd) "a razón de la decisión" respondeel problemajurídicoyeslacausadelaresolución (¿Porquéel Tribunaldecidióde estamanera?)Setratadelosargumentosquejustificandirectamente la decisión. Se construye sacando las premisas fundamentales y conectando las lógicamente (¡nosetratadecopiarypegarextractosdela decisión!)
Se trata de la "razón de la decisión". Responde el problema jurídico y es la causa del resuelve (¿Por qué el Tribunal decidió de esta manera?) Se trata de una construcción lógica que realiza el Tribunal para desarrollar las premisas que fundamentan la decisión. En otras palabras, se trata del ARGUMENTO que justifica directamente la decisión. Construida sacando las premisas fundamentales y conectándolas lógicamente **¡no se trata de copiar y pegar extractos de la decisión!** De hecho, es posible que la corporación esté insistentemente reiterando una misma idea –puede que haya muchos párrafos escritos aunque sólo pueda sacarse una sola premisa de allí. Una misma sentencia puede tener tantas *ratio decidendi*, cuantos problemas jurídicos hayan sido resueltos por el Tribunal. Sin embargo, habrá una ratio decidendi principal de acuerdo al tema por el cual se analice.

3. ARGUMENTOS NO ESENCIALESS(ideasclaras;frasescortas.Usamos viñetas)
3.1. OBITER DICTA RESALTABLES (od): "dichos de paso"; argumentos teóricos,históricos,doctrinalesquesibiennojustificandirectamente ladecisión,lepermiten (al Tribunal Supremo) reforzaroejemplificarsuargumentación. (Sólo losresaltables)
Los obiter dicta, o"dichos de paso" son consideraciones (de tipo teórico, doctrinario, histórico, extra-jurídico, etc.) usadas para fortalecer la argumentación de la decisión. Se trata de ideas que si bien pueden ser importantes o interesantes y refuerzan el argumento, no justifican directamente la decisión.
3.2.INTERVENCIONES (principales argumentos)
Indicaremos aquí en frases cortas y viñetas, los **principales** argumentos de los intervinientes. Sólo incluiremos los argumentos más resaltables relatados.
3.3.VOTO PARTICULAR (SV)(principales argumentos)
Extraeremos aquí los principales argumentos de los votos particulares, si los hay. Los votos Particulares se presentan cuando un magistrado se encuentra en desacuerdo con la decisión tomada por la sala. En ese evento, el magistrado debe esgrimir su desacuerdo en un escrito separado que se encuentra al final del documento, después del "Resuelve"aprobado por la mayoría y de las aclaraciones de voto, si las hay. Los votos Particulares pueden ser totales o parciales, dependiendo de si el magistrado se encuentra total o parcialmente en desacuerdo con lo decidido.

ANEXO VI

PREGUNTAS DE LAS ENTREVISTAS

PREGUNTAS ENTREVISTA: PROFESOR DR. JOSÉ FONTES

TEMA: DERECHO, LA CONSTITUCION Y LEYES ANTITERRORISTAS

TÍTULO: ACTUALIDAD LEGISLATIVA CIBERTERRORISTA EN LA UNIÓN EUROPEA

1. (Aspectos legales). 24 años después del tratado de Maastricht y la creación de la Unión Europea, ¿Cree que las constituciones especificas de cada país Europeo y como ejemplo la Portuguesa, está para actualizar tras la revolución mundial que ha supuesto el fenómeno de Internet? ¿Qué apartados son los que necesitan de esta modernización? ¿Cree que debería haber una única constitución europea?

2. (Aspectos legales). ¿Cree que las últimas actualizaciones en materia penal antiterrorista realizadas tanto en el código Penal portugués como en las leyes europeas con tendencia a estandarizar las leyes en la materia, son suficientes o deben desarrollarse más y estar siempre en constante evolución a la vez que los delitos?

3. (Aspectos legales). Según su opinión y lo acontecido en los últimos años tanto en el mundo y específicamente en Europa ¿Hay necesidad de reglamentar una ley europea de seguridad antiterrorista cibernética?

PREGUNTAS ENTREVISTA: CORONEL NUNO CORREIA BARRENTO DE LEMOS PIRES

TEMA: TERRORISMO, LEYES Y OPERATIVA

TÍTULO: ACTUALIDAD TERRORISTA Y OPERATIVA EN PORTUGAL Y LA UNIÓN EUROPEA.

1. (Aspectos legales). En su opinión, las fuerzas de seguridad ¿encuentran obstáculos legales a la hora de actuar contra una acción terrorista? ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?

2. (Aspectos legales). En su opinión, ¿cuáles son los delitos terroristas más frecuentes? ¿Cree que los terroristas conocen las leyes sobre terrorismo y sus actualizaciones?

3. (Aspectos generales) En su opinión, ¿Qué tipo de amenaza terrorista considera más probable y peligrosa? ¿Considera adecuadas y suficientes las opciones de denuncia y aviso en caso de un posible delito terrorista, a disposición del ciudadano?, ¿Cree que el operativo en caso de ataque, es lo suficientemente ágil?

4. (Aspectos legales). Después de los últimos atentados de Londres y Barcelona, ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?

5. (Aspectos operativos) ¿Considera que Portugal está preparado para la ciberdefensa? ¿Qué opina de la cooperación en materia ciberterrorista de los países de UE y los países de la OTAN?

6. (Aspectos legales). Según su opinión y lo acontecido en los últimos años tanto en el mundo y específicamente en Europa ¿Hay necesidad de reglamentar una ley europea de seguridad antiterrorista cibernética?

PREGUNTAS ENTREVISTA: PROFESORA DRA. SOFÍA CASIMIRO

TEMA: DERECHO Y LEYES ANTITERRORISTAS

TÍTULO: ACTUALIDAD LEGISLATIVA CIBERTERRORISTA EN LA UNIÓN EUROPEA

1. (Aspectos legales). En su opinión, ¿cuáles son los delitos terroristas más frecuentes? ¿Cree que los terroristas conocen las leyes sobre terrorismo y sus actualizaciones?

2. (Aspectos legales). Después de los últimos atentados de Londres y Barcelona, ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?

3. (Aspectos legales). Según su opinión y lo acontecido en los últimos años tanto en el mundo y específicamente en Europa ¿Hay necesidad de reglamentar una ley europea de seguridad antiterrorista cibernética?

PREGUNTAS ENTREVISTA: DR. MANUEL SILVA VIEIRA (SECRETARÍA: SISTEMA DE SEGURIDAD INTERNA)

TEMA: DERECHO, LEYES Y OPERATIVA ANTITERRORISTAS

TÍTULO: ACTUALIDAD TERRORISTA Y OPERATIVA EN PORTUGAL Y LA Y LA UNIÓN EUROPEA.

1. (Aspectos legales). Después de los últimos atentados de Londres y Barcelona, ¿Cree que deberían estar más especializados en materia antiterrorista los Jueces y Fiscales para poder actuar con máxima eficacia y rapidez?

2. (Aspectos generales) En su opinión, ¿Qué tipo de amenaza terrorista considera más probable y peligrosa? ¿Considera adecuadas y suficientes las opciones de denuncia y aviso en caso de un posible delito terrorista, a disposición del ciudadano?, ¿Cree que el operativo en caso de ataque, es lo suficientemente ágil?

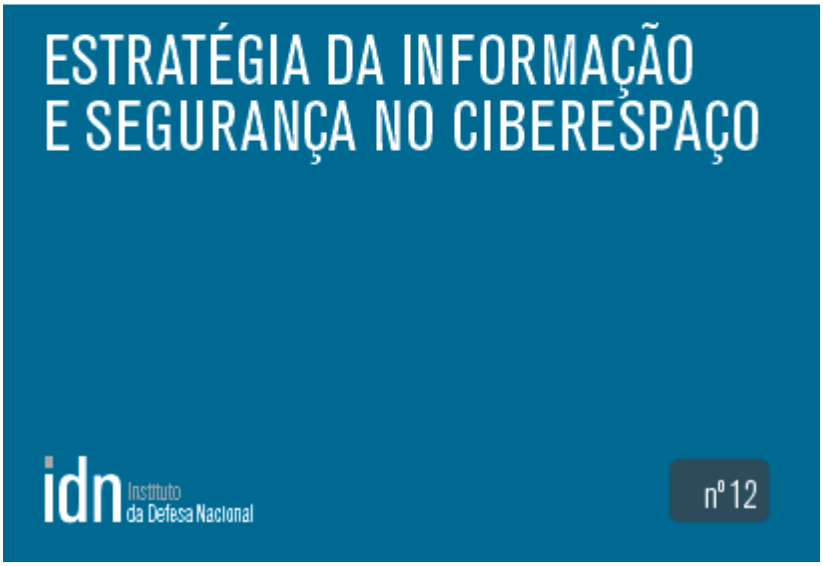
3. (Aspectos operativos) ¿Considera que Portugal está preparado para la ciberdefensa? ¿Qué opina de la cooperación en materia ciberterrorista de los países de UE y los países de la OTAN?

ANEXO VII

ESTRATÉGIA DA INFORMAÇÃO

E SEGURANÇA NO CIBERESPAÇO

idn cadernos

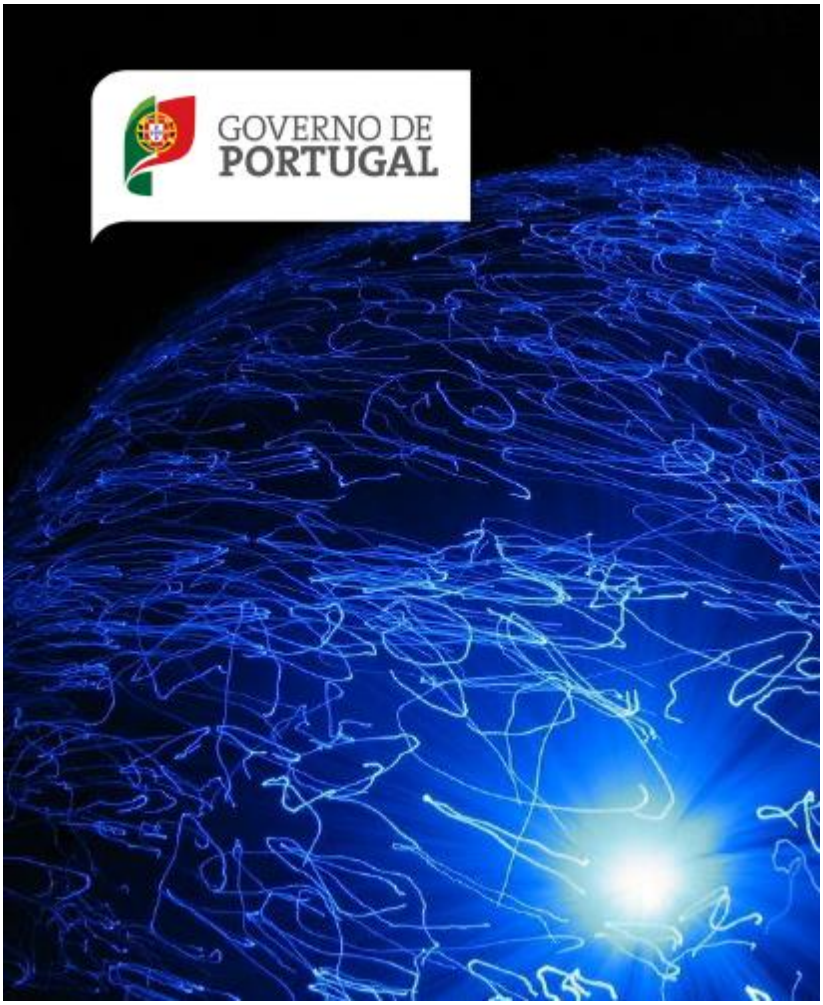


Instituto de Defensa Nacional, diciembre de 2013

https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

ANEXO VIII

NATIONAL CYBERSPACE SECURITY STRATEGY (PORTUGAL)



Estrategia de Seguridad Nacional del Ciberespacio (Portugal)

PRESIDENCY OF THE COUNCIL OF MINISTERS

Resolution of the Council of Ministers 36/2015

In accordance to with articles 199 (d)(f)(g) and 200 (1a) of the Portuguese Constitution, the Council of Ministers resolves to:

1. Approve the National Cyberspace Security Strategy, which is appended to and forms part of this current resolution.

2. Establish that the current resolution takes effect on the date of its approval.

<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf>