EL CRIMINALISTA DIGITAL
PAPELES DE CRIMINOLOGÍA - 2ª ÉPOCA

II Época, Número 10, 2022, pp. 17-37
ISSN 2340-6046

LA DIGITALIZACIÓN DEL MIEDO: DEL TERRORISMO "CLÁSICO" AL TERRORISMO "TECNOLÓGICO"

The fear digitization: from "classical" terrorism to "technological" terrorism

Samar Violeta Francisco Agra*

Resumen
El terrorismo ha mutado con la eclosión tecnológica. Los entornos digitales han fortalecido la interconexión y capacitación de los grupos terroristas. La tecnología ha permitido tender puentes que facilitan las distintas fases y facetas de la criminalidad terrorista: desde la preparación y difusión de ideales hasta la perpetración y ejecución de ataques. Por eso, conviene analizar este fenómeno desde una perspectiva jurídica, pero a partir de la realidad práctica. Tan cambiante y adaptable como siempre ha sido, el terrorismo obliga a mantener la vista fija sobre el y dirigir importantes esfuerzos a crear y fortalecer las infraestructuras (incluso informáticas) que puedan combatir esta férrea amenaza global.

Palabras clave
Terrorismo, Nuevas Tecnologías, Globalización, Redes Sociales, Dark Web, Ciberseguridad, Ciberdelincuencia.

Abstract
Terrorism has mutated with the technological explosion. Digital environments have strengthened the interconnection and training of terrorist groups. Technology has made it possible to build bridges that facilitate the different phases and facets of terrorist crime: from the preparation and dissemination of ideals to the perpetration and execution of attacks. That is why it is convenient to analyze this phenomenon from a legal perspective, but from the practical reality. As changeable and adaptable as it has always been, terrorism forces us to keep an eye on it and direct significant efforts to create and strengthen the infrastructures (including IT) that can combat this fierce global threat.

Keywords
Terrorism, New Technologies, Globalization, Social Networks, Dark Web, Cybersecurity, Cybercrime.

Información del artículo:
Fecha de recepción: 15/12/2022
Fecha de aceptación: 19/12/2022

Cómo citar este artículo:
Francisco Agra, S.V. (2022). La digitalización del miedo: del terrorismo "clásico" al terrorismo "tecnológico", *El Criminalista Digital*, 10, 17-37.

* Contratada predoctoral FPU (ref. FPU21/05642). Departamento de Derecho Penal. Universidad de Granada.

I. Planteamiento

La eclosión de las tecnologías modernas ha revolucionado la vida de las sociedades. No obstante, paralelamente a los beneficios que ha supuesto, estos avances han facilitado y mutado la comisión de delitos. Estas conductas criminales han dado lugar a incesantes debates jurídicos y políticos dirigidos a canalizar tales actos.

Ejemplo de ello es el caso del terrorismo que ha encontrado en el Internet y en los adelantos tecnológicos grandes beneficios y facilidades. El fenómeno terrorista existiría aún sin las nuevas tecnologías, pero no el terrorismo que se conoce hoy en día. La manera de incitar, reclutar, financiar o planificar actos terroristas ha sufrido importantísimos cambios a lo largo de la historia y, uno de los más notorios va de la mano con el crecimiento vertiginoso de instrumentos y estructuras digitales.

El terrorismo ha ido transformándose en un crimen transnacional, amenazante y permanente. Esto ha exigido un Derecho penal que enmarque un proceso de justicia eficiente y legítimo. Una respuesta penal eficaz ya no se proyecta solo en castigar los delitos terroristas, sino en llegar a un estadio previo. Y es que, las redes virtuales suponen un espacio sin fronteras para que las organizaciones terroristas reúnan allí sus ideales y planes, lo que dificulta su identificación, prevención y control.

La presente investigación pretende exponer dichos cambios desde una perspectiva jurídica y práctica, con la intención de llegar a conclusiones y recomendaciones al respecto. Considerando los estragos que ha causado el terrorismo en el mundo, la reacción penal debe ser contundente. Por ello, se debe considerar la actualización y mejora de la regulación penal existente, con el fin de que la legislación antiterrorista sea eficaz y útil y; especialmente, se debe incidir en la necesidad de acompañar el Derecho con la propia ciencia informática para poder hacer frente a este peligro global.

II. El concepto *binario* del terrorismo en el Código Penal Español

Al margen de las dificultades conceptuales en torno al terrorismo, el Código Penal español define lo que se ha de entender por tal, a efectos de su regulación[1]. De ello se encarga el art. 573.1 CP. En su dicción se promueve que el delito de terrorismo será aquel que suponga la comisión de determinados delitos *graves*[2], siempre que se lleven a cabo con alguna de las finalidades siguientes[3]:

[1] El terrorismo no ha recibido un concepto univoco, válido a nivel internacional y que abarque todas las modalidades posibles. *Vid.* FRANCISCO AGRA, S. Una aproximación al (ciber) terrorismo: Modelos previos y actuales. En DOCRIM: Revista Científica, Nº 8, 2021. Asimismo, sobre la problemática general de la construcción jurídica del concepto de terrorismo en la regulación positiva española, *vid.* CANCIO MELIÁ, M. El concepto jurídico-penal del terrorismo entre la negación y la resignación. En Terrorismo, sistema penal y derechos fundamentales. Alberto Alonso Rimo, María Luisa Cuerda & vv.aa (dir), 2018.

[2] Especifica como delitos graves los cometidos "*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, de falsedad documental, 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*". La reforma del Código Penal operada por la Ley Orgánica 1/2019 de 20 de febrero, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, y abordar cuestiones de índole internacional, añade en este inciso la *falsedad documental*, con el fin de promover la literalidad de la Directiva europea y armonizar la definición de los delitos terroristas en los distintos países de la Unión (véase la Proposición de Ley Orgánica Nº 624/000016). *Vid.* LAMARCA PÉREZ, C. Tema 25. Delitos contra el orden público. En Delitos. La parte especial del Derecho Penal. Editorial Dykinson, 2019. La penalista explica que se trata de tipos pluriofensivos donde se vulneran bienes jurídicos individuales de forma inmediata, a la vez que se protegen bienes jurídicos colectivos de forma mediata.

[3] El hecho de que el Código Penal indique que el delito de terrorismo requiere *alguna* de las finalidades mencionadas, deja claro que basta con que tenga lugar *una* de ellas.

La subversión del orden constitucional, la supresión o desestabilización grave del funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, o la obligación a los poderes públicos a que realicen o se abstengan de realizar un acto**:** La subversión del orden constitucional es, en realidad, una expresión jurídica indeterminada. Ni en el Código ni en legislaciones especificas complementarias se interpreta lo que debe entenderse a estos efectos. Se entiende como un intento de cambiar o destruir el orden constitucional imperante y establecido, con violencia y desafío hacia el Estado (GARRIDO, Á., 2015). No obstante, es un concepto que requiere aclaraciones interpretativas. LAMARCA PÉREZ & MIRA BENAVENT (2013: 43) consideran que tal subversión no debe resumirse solo a una sustitución del sistema político sino que, desde una perspectiva penal, lo que interesa es la violencia utilizada por la organización terrorista para conseguirlo.

Que se haga referencia a una finalidad política como la subversión del orden constitucional o la desestabilización grave de instituciones políticas no supone alteración alguna de lo dictado por la Constitución Española en su art. 13. Los delitos de terrorismo no son considerados como delitos políticos, pero tampoco se podría asumir que son absolutamente apolíticos[4]. El terrorismo ha ido progresando hacia el intento de satisfacer objetivos cada vez más alejados de la política y la ideología y eso no lo hace menos terrorismo[5].

La inclusión de la desestabilización del funcionamiento de estructuras sociales y económicas como finalidad terrorista –no solo políticas- evidencia los distintos factores que se ven expuestos antes estos ataques radicalizados y las diversas modalidades subjetivas que les pueden acompañar.

La alteración de la paz pública**:** Este inciso ha sido cuestionado por un importante sector de la doctrina española, en la medida en que también se trata de un concepto jurídico indeterminado. Para este grupo de juristas, la "paz pública" puede dar lugar a un bien jurídico que amplíe el tipo penal a través de una subjetivación incompatible con el principio del hecho (CANCIO MELIÁ, M., 2010: 115 y ss.). Ante esta indefinición también hay posturas intermedias, que intentan concretar el mencionado bien jurídico. En esta dirección transita ASUA BATARRITA (2006), quien considera que la referencia a la paz pública solo es aceptable como expresión de la "*seguridad cognitiva*" en relación con distintos bienes jurídicos amenazados.

Por su parte, el Tribunal Supremo ha definido la paz pública como la "*tranquilidad o sosiego ciudadanos*" o "*el sosiego de amplios sectores de población que se ven conmocionados por las tácticas terroristas*"[6]. Se trataría, entonces, de un concepto distinto al de orden público, que es más amplio.

La desestabilización grave del funcionamiento de una organización internacional**:** Con este apartado el Legislador penal procuraba dotar a la regulación de un carácter más internacional, equiparando las instituciones y administraciones del Estado español con las internacionales y supranacionales (AZNAR, J., 2016).

La provocación de un estado de terror en la población o en una parte de ella: Implica generar una intimidación grave a la población, siendo este el efecto característico del fenómeno terrorista, fundamentado en su carácter sistemático, reiterado e indiscriminado. De hecho, la existencia misma de una organización estable cuyo fin sea la planificación y ejecución de delitos de esta naturaleza ya es un factor desestabilizante o amenazante para la población en sí mismo (ASUA BATARRITA, A., 2002). De esta forma, el terror no es tanto un objetivo en sí mismo, sino un instrumento para llegar a un fin.

[4] Aun cuando las acciones terroristas no se dirijan contra el Estado, igualmente modifican su comportamiento por los efectos que resultan (Andrade, O.D., 2015: 69).

[5] *Vid.* JAKOBS, G. . Derecho Penal del Enemigo. Thomson Civitas, Cuadernos Civitas, 2003; quien afirma que la teoría del Derecho Penal del Enemigo entiende que la identidad del terrorista puede equipararse a distintas pertenencias, no solo políticas, por lo que "*se torna irreductible y esencialista y justifica la radicalización del antagonismo hasta las últimas consecuencias*".

[6] *Vid.* SSTS, Sala Segunda, de 25 de mayo de 1976 y de 30 de enero de 1975, respectivamente.

No obstante, el *terror* o el *miedo* es un concepto que, en este contexto, requiere particularidades[7]. LÓPEZ CALERA (2002: 54 y 55) señala interesantes ideas a este respecto. En primer lugar, concluye que no puede tratarse de terrores aislados o individualizados, como el que una mujer puede sentir ante amenazas constantes por su pareja sentimental[8]. En segundo lugar, afirma la necesidad de que el terror generado por un comportamiento o actividad terrorista tenga una permanencia en el tiempo. Aunque los "*lobos solitarios*" o los individuos que se autoadoctrinan por su cuenta perpetran hechos aislados *per se*, igualmente se adscriben a ideales terroristas previos y sostenidos en el tiempo[9]. Y en tercer lugar, el filósofo caracteriza al terrorismo con una violencia que no discrimina a sus víctimas.

Resulta claro que la fórmula seguida en la legislación penal española para conceptualizar los delitos terroristas es la siguiente:

delito *grave* + *una* o *varias* finalidades= delito terrorista.

La conjunción de los factores de tal fórmula produce como resultado la interacción de elementos objetivos y subjetivos en el injusto, algunos muy vagos e indeterminados. Pero, además de ello, se ha advertido la inclusión de un catálogo de delitos que, si bien han sido calificados como graves, en realidad son muy dispares entre sí. Por ejemplo, equipara en gravedad, a estos efectos, los delitos contra la vida con el de falsedad documental; añadido éste último con la reforma del Código Penal de 2019.

Esto no es en sí mismo un problema, puesto que todos los delitos son sumamente graves en un contexto terrorista -aunque los daños personales siempre sean los más gravosos-, salvo que la regulación se exceda ampliando innecesariamente la lista de delitos del art. 573.1 CP. De hecho, se incluyen más comportamientos ilícitos en su dicción que en los Convenios internacionales, como lo ilustra el caso de la libertad o integridad sexuales. Incluso, la finalidad de alterar la paz pública tampoco está incluida en la Directiva (UE) 2017/541.

Es notorio que la tipificación penal en España va unos pasos más allá que los lineamientos europeos e internacionales, quizá por su dura experiencia con el terrorismo. Se debe insistir en que no es algo necesariamente malo, pero sí que merece atención, en la medida en que la ampliación de las barreras punitivas es uno de los caracteres del Derecho penal del enemigo y, sin duda, debe estar sujeto a control.

Ahora bien, la concepción de los delitos de terrorismo en el Código Penal adquiere una construcción *binaria*[10], atendiendo a lo establecido en el segundo apartado del art. 573 CP, donde se expone lo siguiente: "*se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a*

[7] La ausencia de estas precisiones puede conducir a ver como terrorista lo que verdaderamente no lo es. Por ejemplo, peligrosamente, el Tribunal Constitucional español afirma que no se puede excluir la posibilidad de que determinados grupos u organizaciones criminales, sin necesidad de que tengan un objetivo político, puedan crear una situación de alarma y, en consecuencia, una situación de emergencia social "*que autoriza (o legitima) a equipararlos a los grupos terroristas propiamente dichos*" (STC 199/1987, FJ 4).

[8] Llama la atención que el autor, que escribe el artículo citado en 2002, apunta que nadie llama a la violencia doméstica como "terrorismo". Hoy es frecuente escuchar esta referencia, especialmente en medios de comunicación, lo cual evidencia cómo el "terrorismo" puede ser un término convertido en una especie de *eslogan* para dotar de un mayor reproche a conductas que, en sí mismas, son totalmente inaceptables a nivel social y jurídico-penal.

[9] Un importante sector doctrinal considera que no es viable la aceptación de "terroristas individuales", en la medida en que no es plausible que un sujeto por libre y sin la cobertura de una organización terrorista pueda conseguir éxito en su ataque. Sin embargo, desde un punto de vista teórico y atendiendo al alcance y el poder de destrucción de ciertas armas, sí es posible. *Vid.* LLOBET ANGLÍ, M., Lobos solitarios yihadistas: ¿terroristas, asesinos o creyentes? Retorno a un Derecho penal de autor. En Actas VII Jornadas de Estudios de Seguridad, Colección de Investigación, Instituto Universitario General Gutiérrez Mellado, 2015.

[10] *Vid.* LAMARCA PÉREZ, C. Tratamiento jurídico del terrorismo. Ministerio de Justicia, Secretaría General Técnica, 1985. La autora entiende que el terrorismo se trata de una noción genérica y que abarca manifestaciones delictivas de diversa naturaleza. En función de ello, señala la necesidad de clasificar, es decir, "*de distinguir las diversas modalidades que caben dentro de esa noción generica*". Cabría analizar, si la dicción del Código conduce a, al menos, una clasificación inicial entre el terrorismo tradicional y el cibernético.

264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior". Se trata de una referencia explícita del terrorismo cibernético[11].

De acuerdo con el Consejo de Europa, esta forma de terrorismo hace referencia al "*que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos*"[12]. Sin embargo, hoy es una apreciación que se queda corta. El terrorismo se vale de la tecnología ya no solo como medio sino también como fin. No necesariamente utiliza las tecnologías de la información y la comunicación (TIC) como vehículo para cometer delitos terroristas tradicionales, sino que, en función del art. 573.2 CP, obstaculizar o interrumpir sin autorización el funcionamiento de un sistema informático ajeno, siempre que tenga como finalidad alguna de las analizadas, por ejemplo, será un delito terrorista en sí mismo (art. 264 bis CP).

El ciberespacio ha sido definido como un espacio de dominio artificial construido por el hombre, diferenciado de los otros dominios de guerra: tierra, aire, mar y espacio. Al no estar aislado, el ciberespacio está profundamente vinculado y apoyado por medios físicos, por lo que, atacar tal interconexión puede tener consecuencias muy graves en la seguridad nacional e internacional (GAMÓN, V., 2017).

Por tanto, aunque la redacción del art. 573 CP transmite la idea de querer proteger este dominio digital de los ataques terroristas, no siempre parece muy práctica tal división binaria que hace a la hora de definir las modalidades del terrorismo. Varios de los delitos incluidos en el primer apartado pueden perpetrarse a través de medios tecnológicos y serían terrorismo. Y los delitos informáticos cometidos con finalidades terroristas también serían plenamente terrorismo aunque el ciberespacio sea el destinatario de ese ataque. Así, lo que parece que pretende ser una diferenciación entre el terrorismo tradicional y el cibernético en realidad acaba bifurcando este último innecesariamente.

La redacción del precepto podría incluir los delitos informáticos dentro del primer apartado -en la medida en que son delitos graves que pueden ser realizados con finalidades terroristas-, o bien, podría aclararse en el primer apartado que dichos delitos pueden ser cometidos también por vías tecnológicas. Si no se precisa, la lectura del articulo rememora solo al *modus operandi* tradicional del terrorismo.

III. Las organizaciones y grupos terroristas antes y después del Internet

Las organizaciones y grupos terroristas funcionan, bien de forma jerárquica, o bien a través de una *red* extensa y compleja, conformada por, a su vez, más redes: la red de los atentados, la red afectiva, las relaciones internacionales previas y la red con la organización de que se trate (RODRÍGUEZ, J.A., 2004: 158). Aunque también pueden combinar ambas estrategias. Esto es aún más espinoso si se considera la amplia serie de amenazas que pretenden abarcar los terroristas; desde los "*lobos solitarios*" radicalizados, hasta el terrorismo organizado en zonas de conflicto con combatientes extranjeros.

La estructura organizativa jerárquica se ha caracterizado por poseer en su seno una definida cadena vertical de control y mando. Las órdenes se pasean entre los miembros de arriba hacia abajo, pero no necesariamente de manera horizontal. Por esta razón, solo los líderes o la alta dirección tienen una visión general de la organización, generalmente con especialización de funciones. Sin embargo, como refleja SOMIEDO (2015), este orden era muy vulnerable por ser fácilmente interceptable por los servicios de inteligencia. Ahora bien, operar en células independientes dificultaría la comunicación entre sí para la planificación de atentados masivos

[11] El ciberterrorismo también adolece de un concepto admitido con carácter general. Y no es de extrañar pues, como menciona FERNÁNDEZ HERNÁNDEZ, "*si no se ha fijado qué es terrorismo, lógico es que tampoco sea posible encontrar una definición inequívoca de qué debe entenderse por ciberterrorismo*".

[12] Citado en SUBIJANA, I.J. *El ciberterrorismo: una perspectiva legal y judicial.* Eguzkilore, Nº 22, 2008. El Magistrado destaca en su artículo que los medios tecnológicos, entre otras cosas, favorecen la ejecución trasnacional del hecho y los efectos deletéreos sobre núcleos significativos de personas o detrimentos sobre infraestructuras públicas o servicios comunitarios básicos; así como dificultan la obtención de fuentes de prueba relativas a la comisión y su autoría.

y simultáneos. Era un obstáculo complicado para los terroristas, que las nuevas tecnologías les han ayudado a sortear.

Así es como el Internet revolucionó el esquema que tenían las organizaciones y grupos terroristas. Esta infraestructura virtual ha servido como herramienta potenciadora del fenómeno. Lo cual no quiere decir que las TICs sean el problema porque, como se ha adelantado, aún sin ellas, por la adaptabilidad del terrorismo, este fenómeno seguiría existiendo. No obstante, su utilización por las organizaciones terroristas ha supuesto una novedosa y práctica estrategia comunicativa, que debe ser atendida y estudiada constantemente en el marco de la lucha antiterrorista.

Siendo Internet la mayor plataforma de expresión a nivel mundial, los terroristas se han ido volcando hacia él. La Prof. SÁNCHEZ MEDERO (2010: 204 y ss.) ha desarrollado una tipología de sitios web en los que los terroristas se han ido manifestando:

a. Sitios oficiales o webs de la organización terrorista. Se trata de páginas "oficiales" creadas específicamente para la difusión de contenidos terroristas dotados de un carácter más "institucional".

   Un ejemplo de estas páginas fue la revista en línea *DABIQ*, editada por *Al Hayat Media* para explicar y proyectar el proyecto del Estado Islámico. Más que dirigirse a un colectivo musulmán, como se llegó a pensar en algún momento, el que el título de cada número apareciera en inglés permite notar que el destinatario era un grupo más amplio y heterogéneo de personas. Con una estructura organizada, el contenido de la publicación *web* abarcaba crónicas, artículos, entrevistas, experiencias, reportes históricos, consejos para las mujeres, discursos de enemistad, entre otros (MARTÍN, M.A., 2020). No obstante, se evidencia su corta permanencia al tomar en cuenta que *DABIQ* y *Rumiyah*[13] no llegan, ni conjuntamente, a los 30 números.

   Evidentemente, constituyen el grupo de perfiles *online* más cuidados por la organización, pero también los más perseguidos por los servicios de seguridad, por lo que su presencia es bastante breve. Ante esto, la solución de los terroristas es transmitir y editar su mensaje y sus materiales mediante foros y webs de confianza (TORRES SORIANO, M., 2009).

b. Foros. En estos portales online se pretende generar debates a partir de preguntas sobre ciertos temas. Resulta muy atractivo para las organizaciones terroristas para colgar comunicados y enlaces de nuevos materiales (Torres Soriano, M., 2007), por lo que suelen dotarlos de mayor "seguridad" mediante contraseñas de entrada o censura interna por parte de los administradores.

   La creación de estos puentes comunicacionales al servicio de objetivos terroristas supuso en su momento una amplia red propagandística ramificada y carente de relaciones verticales, aunque respetuosas de una marcada jerarquía (CANO PAÑOS, M.A., 2019). El consumo de contenidos terroristas se impulsa en estas plataformas por su alcance mundial y su fácil accesibilidad, si bien suelen preferir los foros cerrados. Y si el Internet puede favorecer el refuerzo emocional de los terroristas, cuánto más se potencia esto si el que se acerca ve un debate abierto e inclusivo que proporciona "unión" en una misma causa, desdibujando fronteras físicas.

c. *Blogs*. Son espacios virtuales públicos en el que las personas pueden exponer abiertamente su opinión, así como publicar contenidos y enlaces a otras páginas. Permiten un *feed back* abierto y poco controlable, en la medida en que fácilmente se pueden crear identidades o perfiles falsos para acceder a ellos desde cualquier ordenador.

[13] Como sucesora de la revista *DABIQ,* fue publicada en ocho idiomas distintos para fomentar la violencia y el reclutamiento de seguidores a través de propaganda religiosa manipulada (Colomo, M.I., 2016), incluyendo consejos para perpetrar ataques en países occidentales.

El objetivo principal de los *blogs* es alcanzar un posicionamiento o una referencia para el público que consume los artículos, opiniones e información disponibles en ellos (MEMBIELA, M. & PEDREIRA, N., 2019). En las manos equivocadas, como la de los terroristas, pasaría de ser un medio democrático para intercambiar opiniones o difundir un producto a ser impulsor de ideologías y pensamientos radicales. Su fácil adaptación a la comunidad y su sencilla accesibilidad son valoradas por los terroristas para el desarrollo de sus actividades.

d. Redes de distribución de contenidos: Son redes de servidores distribuidas en centros de datos a nivel mundial con el fin de almacenar una copia de un sitio web. Es la estrategia *online* emprendida por los terroristas para asegurarse de que, aún siendo víctimas de *hackeos*, puedan conservar su infraestructura (TORRES SORIANO, M., 2007: 261). Sin embargo, también son utilizadas por los terroristas como directorio actualizado de páginas webs terroristas.

Finalmente, la Profesora clasifica las redes sociales. Sin embargo, estas serán objeto de un análisis más profundo en lo que prosigue de este artículo. Lo que procede destacar desde ya es la forma en que todas estas estructuras digitales ponen sobre la mesa nuevas oportunidades a los terroristas. Su esquema de funcionamiento ha cambiado completamente gracias a ellas, por lo que la respuesta penal a semejante actividad delictiva debe asegurarse de estar actualizada; al corriente de tales avances. Es lo que se evidencia en la redacción actual del Código Penal, que intenta ofrecer un tratamiento diferenciado al *ciberterrorismo* en los distintos tipos delictivos terroristas. Ahora bien, no siempre se logra de una manera integrada y natural en su dicción, sino que transmite un cierto desorden y confusión en algunos casos.

IV. Las figuras delictivas terroristas y las nuevas tecnologías

1. El delito de adoctrinamiento o adiestramiento terrorista

El art. 575 CP tipifica el adoctrinamiento o adiestramiento pasivo. Este delito sufre una interesantísima transformación tras la reforma del Código Penal español operada por la Ley Orgánica 2/2015, pasando a alcanzar al receptor -ya no solo al facilitador- de la capacitación en materia terrorista. Así, el sujeto pasivo de las labores de proselitismo y formación terrorista pasa a ser el sujeto activo de un delito penal autónomo, cuya ubicación sistemática ni siquiera permite su inclusión formal dentro de los delitos de colaboración terrorista (OLMEDO, M., 2015: 1436).

Sin duda, la estructura de este novedoso delito supone un amplio adelantamiento de la punibilidad en lo que respecta al fenómeno terrorista, por su especial peligrosidad y que hace eco, nuevamente, de las ideas de JAKOBS (2003: 40) en su teoría del Derecho penal del enemigo: "*la punibilidad se adelanta un gran trecho hacia el ámbito de la preparación, y la pena se dirige frente a hechos futuros*"[14]. De forma que, lo que objetivamente constituiría un hecho preparatorio en otro delito y frente a las reglas de los arts. 17 y 18 CP, en este marco se trata de un tipo delictivo autónomo.

Es decir, si el adiestramiento se realiza sin que incurra en la comisión concreta de algún delito terrorista, se trata de un injusto con sustantividad propia; distinto a lo que ocurre si desemboca en la perpetración de

[14] En este sentido, *vid.* LLOBET ANGLÍ, M. ¿Terrorismo o terrorismos?: Sujetos peligrosos, malvados y enemigos. Revista Jurídica, Nº 31, Universidad Autónoma de Madrid, 2015. La jurista aclara que la agravación en sí de los delitos de terrorismo no conforma el arsenal punitivo del Derecho Penal del enemigo, pero cuestión distinta es lo relativo a cuánto más hay que castigar y cómo hacerlo. De forma que, "*se vulneran los principios de proporcionalidad y culpabilidad en el "cuánto más" y en el "cómo" castigarlos, puesto que, en ocasiones no se toma en cuenta la gravedad del hecho y se antepone el tipo de autores a la clase de actos concretos cometidos*"; por lo que el problema surge cuando la agravación desborda los límites del injusto. También *vid.* POLAINO-ORTS Derecho Penal del Enemigo. Fundamentos, potencial de sentido y límites de vigencia. Bosch, 1ª Edición, 2009, que resume la doctrina jakobsiana en un concepto de enemigo, afirmando que lo es "*quien, incluso manteniendo intactas sus capacidades intelectiva y volitiva, y disponiendo de todas las posibilidades de adecuar su comportamiento a la norma, decide motu propio autoexcluirse del sistema, rechazando las normas dirigidas a personas razonables y competentes, y despersonalizándose a sí mismo mediante la manifestación exterior de una amenaza en forma de inseguridad cognitiva, que –precisamente por poner en peligro los pilares de la estructura social y el desarrollo integral del resto de ciudadanos ('personas en Derecho')- ha de ser combatida por el Ordenamiento jurídico de forma especialmente drástica, con una reacción asegurativa más eficaz. Esta reacción se circunscribe a garantizar y restablecer el mino de respeto para la convivencia social: el comportamiento como persona en Derecho, el respeto de las demás personas y –en consecuencia- la garantía de la seguridad cognitiva de los ciudadanos en la norma*".

alguna de las conductas terroristas tipificadas en el Código Penal, en cuyo caso el autoadoctrinamiento se absorbe con la autoría o participación del delito de que se trate (OLMEDO, M., 2015: 1435).

Muy acertadamente la regulación penal ya no considera solo el mundo físico, al castigar el adoctrinamiento militar o de combate -específicamente en lo relacionado con las armas químicas-, o la adquisición o posesión de documentos idóneos o dirigidos a la incorporación o colaboración con grupos u organizaciones terroristas; sino también el *ciberespacio.* El espacio virtual ofrece un sinfín de recursos de información que permiten la radicalización a distancia y sin ningún control.

Atendiendo a lo previo, el precepto menciona textualmente que "*se entenderá que comete este delito quien 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*" (art. 575.2 CP). Es una clara manera de exponer la mutación que ha sufrido la radicalización terrorista, pasando de producirse en entornos físicos -como las prisiones o la movilización a zonas de conflicto- a entornos virtuales y de acceso instantáneo. A través de la red se produce un entrenamiento virtual enmarcado en una comunicación directa y ausente de intermediarios para difundir el mensaje extremista (MORENO, J.D., 2017: 349 y ss.).

Por su reciente incorporación en el catálogo de comportamientos punibles, el desarrollo jurisprudencial es aún bastante escaso. No obstante, entre las sentencias que existen al respecto se halla la Nº 354/2017, emitida por la Sala Segunda de lo Penal del Tribunal Supremo. En ella se aclara que el acceso habitual a Internet o el contenido al que se accede debe estar dirigido o resultar idóneo para incitar a la incorporación o colaboración con una organización o grupo terrorista o sus fines. Se trata de una exigencia objetiva: "*con la finalidad de capacitarse, donde el logro pretendido de tal aptitud, a su vez, ha de ser para llevar a cabo cualquiera de los delitos tipificados en este Capítulo*" (FJ 2). Siendo así, no basta el contenido de las páginas sea óptimo para capacitar en materia terrorista, sino que deben haber sido consultadas para cometer actos terroristas.

Pero, ¿cómo puede determinarse eso de manera certera en una instancia tan previa? Si se es muy flexible en este punto, el precepto acabaría siendo totalmente inoperante; pero si, por otro lado, se es sumamente rígido a la hora de interpretar esto –que por más que se intente objetivar, es inevitablemente subjetivo- se acabaría poniendo en peligro la libertad ideológica, religiosa y de pensamiento de las personas, es decir, sus esferas más íntimas. El delito de autoadoctrinamiento no se contempla en los instrumentos de la Unión Europea ni es apoyado por el Consejo de Europa y, la regulación española es insuficiente para dar respuesta a esta seria problemática[15].

2. El delito de financiamiento del terrorismo

Los avances tecnológicos han traído consigo un paradigma que favorece el establecimiento de un panorama social de tipo virtual o impersonal, transformando los contextos en que se desenvuelve la comunidad (GONZÁLEZ, L., 1997). Sin menospreciar los múltiples beneficios que conlleva, no deja de ser cierto que el ciberespacio constituye un cosmos sin fronteras con serias dificultades para su control, pudiendo refugiar a criminales y terroristas que han encontrado en aquel una vía libre para perpetrar sus comportamientos delictivos.

Entre otras cosas, las tecnologías del siglo XXI han evidenciado y permitido que se pueda generar terror sin emplear la violencia física (PASTRANA, M.A., 2020: 81). En tanto el mundo digital ofrezca puentes para la ejecución de actividades y negocios maliciosos e ilegales y/o para llevar a cabo acciones coordinadas dirigidas

[15] *Vid.* BAYARRI GARCÍA, C.E. Los nuevos delitos de terrorismo. Adoctrinamiento activo y pasivo vs. enaltecimiento y provocación a la comisión de delitos terroristas. En Terrorismo, sistema penal y derechos fundamentales. Alberto Alonso Rimo, María Luisa Cuerda & vv.aa (dir), 2018. La autora recuerda que una configuración legal como la que se plantea supone graves problemas, por su ambigüedad y extensión y contrasta el tipo penal con lo establecido en la Directiva (UE) de 15 de marzo de 2017 que, según su artículo 8, no abarca el adoctrinamiento meramente ideológico como el que propone el Código Penal español.

a desestabilizar los Estados democráticos y sus instituciones, la seguridad seguirá teniendo muchos retos por delante (PÉREZ, A., 2020: 5).

Aunque posiblemente nunca se alcance una web totalmente libre de este tipo de amenazas, lo que sí es inmutable es la resolución que deben tener las Administraciones del mundo de dirigir importantes esfuerzos a la creación de infraestructuras que puedan combatir la cibercriminalidad. Entre los usos indebidos del Internet y de las TICs destaca recientemente la utilización de las criptomonedas para fines ilícitos. Este tipo de monedas virtuales utilizan tecnología criptográfica, siguiendo protocolos bien definidos, para realizar transacciones de forma expedita y sin limitaciones territoriales, a partir de billeteras digitales que se respaldan por la confianza de las personas (RANGEL, L., 2019: 19).

Los monederos virtuales se han vinculado con el blanqueo de capitales, la evasión fiscal, la compra de servicios y bienes ilícitos y, la financiación de organizaciones con fines terroristas (PÉREZ, D., 2020: 19). En materia de terrorismo, esto ha favorecido la financiación de sus organizaciones, especialmente por el anonimato y la carencia de control descentralizado que caracteriza a dichas transacciones (ESPINOZA, X., NAVARRETE, G. & WONG, E., 2021). Los terroristas encuentran en estos movimientos virtuales de dinero vías sencillas de financiación, para no recurrir a mecanismos más complejos (SÁNCHEZ-GIL, L., 2021: 6).

En vista de lo anterior, dentro de los muchos ámbitos cercados por la legislación antiterrorista, uno de los principales focos de interés es lo relativo a la financiación de este tipo de actividades. Tradicionalmente, las organizaciones terroristas y sus partidarios se han valido de, al menos, cuatro categorías generales para recaudar fondos y recursos a través de la red: la recaudación directa, el comercio electrónico, las contribuciones dirigidas a organizaciones benéficas y los servicios de pago en línea (UNODC, 2013: 7). Con la evolución del mundo digital, los terroristas han ampliado sus horizontes para optimizar su sistema de financiación.

Las criptomonedas y, especialmente el Blockchain[16] que se encuentra tan en auge en la actualidad, han sido una accesible opción para que los terroristas financien sus acciones ilícitas; no solo por su sencillez sino por las dificultades que tienen las autoridades para rastrear o bloquear dichas transacciones. Es uno de los retos jurídicos más actuales en materia terrorista que evidencia, una vez más, la mutación estructural que la tecnología cibernética ha generado en el seno de estas organizaciones. De hecho, en 2019 se produjo la primera sentencia del Tribunal Supremo –la 326/2019- sobre los *bitcoins*, aclarando su singular caracterización jurídica, por lo que el desarrollo jurisprudencial en lo relativo a la utilización de aquellos para financiar el terrorismo aún debe esperar.

Ante la responsabilidad de los Estados de regular este tipo de criptodivisas, no han sido pocos los Gobiernos que han dictado decisiones y emprendido normativas a este respecto, especialmente al detectar la facilidad que supone para el blanqueo de capitales y su, casi inevitable, vinculación con el terrorismo. El caso español ha tenido esto en cuenta, además de en la Ley 10/2010, desde el propio articulado del Código Penal. Es por eso que en el art. 576.1 CP se castiga al 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*"[17].

No es la primera vez que una nueva tecnología supone riesgos potenciales para la seguridad cibernética y de la población, pero al materializarse un cambio en el seno de las estructuras terroristas, el Derecho debe

[16] Es reconocido por algunos expertos como "la nueva generación de Internet", en la medida en que permite transmitir valores de manera descentralizada y segura, con un sistema basado en la confianza. En este sentido, véase DOMINGO, C. Bitcoin, criptomonedas y Blockchain. Editorial Planeta, 2018. También *vid.* PARRONDO, L. Tecnología Blockchain, una nueva era para la empresa. En Revista de Contabilidad y Dirección, Vol. 27, año 2018, pags. 11-31, quien afirma que las principales ventajas de Blockchain son: el intercambio sin intermediación de terceros, la inviolabilidad, la transparencia, el control de usuario, la inmutabilidad, la simplificación del sistema contable y/o las transacciones eficientes.

[17] El apartado 3 del art. 576 contiene una agravación específica del tipo penal relativo a la financiación del terrorismo, cuando se llevase a cabo "*atentando contra el patrimonio, cometiendo extorsión, falsedad documental o mediante la comisión de cualquier otro delito*".

actuar de forma eficiente. En este caso, no basta con que el Código Penal incluya la previsión del ciberterrorismo, sino que sea lo suficientemente actualizada como para dar respuesta a estas nuevas realidades.

No obstante, la regulación normativa que pretenda el control de las transacciones en *Blockchain* serán más adecuadas si se adoptan a nivel internacional, en tanto aquellas no se hayan sujetas a ningún tipo de fronteras territoriales. Asimismo, es esencial remarcar que el control que se dé a las criptomonedas, si se quiere que éstas subsistan, no pude desvirtuar sus facilidades y beneficios.

3. El delito de enaltecimiento terrorista

El delito de enaltecimiento o justificación públicos de los delitos terroristas o de quienes participasen en su ejecución o en la realización de actos que supongan descredito, menosprecio o humillación a las víctimas de tales ataques, se regula en el art. 578 CP. Tal artículo prevé también una referencia expresa del ámbito cibernético al establecer que "*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*" (apdo. 2), se tratará de un subtipo agravado que cualifica la pena en su mitad superior. Además, dice el apartado 3 que cuando el delito se cometiese a través de las TICs se acordará la retirada de los contenidos o servicios ilícitos, pudiendo el Juez, subsidiariamente y en algunos supuestos, pedir esto a los propios prestadores de servicios de alojamiento.

Se trata, entonces, de dos conductas -necesariamente activas, al contener el art. 578 CP una norma prohibitiva- diferenciadas: la apología específica o *in genere* del terrorismo[18] y la humillación o menosprecio de sus víctimas. Para un considerable número de juristas, aquellas no están relacionadas entre sí, por lo que no tiene mucho sentido su tipificación conjunta[19]. De hecho, el propio Tribunal Supremo ha manifestado que la distinta acción típica y los elementos que caracterizan a uno y otro caso aconsejan "*la tipificación separada en artículos diferentes*" (STS 224/2010, FJ 3). Puede que la razón de ser de esta estructura penal se derive de la consideración del Legislador de que son acciones usualmente cumulativas[20]. No obstante, se puede humillar a las víctimas del terrorismo sin que ello tenga que suponer una justificación o enaltecimiento del acto en sí.

Lo cierto es que, en cualquier caso, debe tratarse de una apología del terrorismo pública y dirigida a un destinatarios no individualizables (OLMEDO, M., 2015: 1438), frente a actos de reafirmación interna que no alcanza el Derecho penal. Las vías para hacer llegar ese mensaje a una generalidad de personas también han ido variando con los avances tecnológicos. Por ejemplo, hace casi dos décadas atrás, en homenaje a ETA, se colocó una pancarta de importantes dimensiones en la Plaza vizcaína del Ayuntamiento[21]. Unos años más adelante, en el funeral de un miembro de dicha banda armada, uno de los asistentes presentó un discurso con comentarios elogiosos hacia la actividad terrorista de la organización[22]. Hoy día, la proyección de la apología terrorista tiene un vehículo más masivo, inmediato e indiscriminado que en los casos anteriores.

Es así como las redes sociales se han convertido, en la actualidad, en el punto de mira de la mayoría de los casos de enaltecimiento o justificación del terrorismo. Un detalle que ya de por sí demuestra este cambio es el cuantioso incremento de condenas por el delito analizado, ante las conductas ofensivas habituales en distintas plataformas virtuales de *social media.* Esto ha generado un intenso debate sobre los límites de la libertad de expresión. El alcance de la intervención penal se determina no solo en función de qué castigar sino el cómo y el

[18] Diferenciando que el *enaltecimiento* se refiere a ensalzar o engrandecer el fenómeno terrorista, colocando tales acciones y sus autores como asimilados al orden jurídico, en vez de contradecirlo frontalmente (STS 656/2007); mientras que, la *justificación* implica la argumentación a favor de tales actos e incluirlos como actos permitidos o lícitos, a pesar de constituir un comportamiento criminal (STS 149/2007).

[19] Es el caso, por ejemplo, del Prof. CANCIO MELIÁ (2010: 272), que considera que el Legislador quería disimular un comportamiento cuya criminalización es discutible -el enaltecimiento o justificación del terrorismo-, con uno que no lo parece.

[20] Lo mismo ocurre en el caso de la penalización del discurso negacionista del art. 510 CP, cuyo alcance material hace referencia a la difusión de ideas o doctrinas que *nieguen* o *justifiquen* el delito de genocidio, los delitos de lesa humanidad y los de guerra. Pero también añade en el apartado segundo el castigo por humillar o menospreciar a las víctimas del terrorismo.

[21] Véase, a este respecto, la Sentencia de la Audiencia Nacional de 27 de abril de 2006.

[22] Véase, a este respecto, la Sentencia de la Audiencia Nacional de 23 de marzo de 2007.

cuánto (MIRÓ LLINARES, F., 2015: 19). Por eso, resulta complejo determinar con claridad lo que constituye una ofensa y lo que no.

En un intento por delimitar el punto de inflexión entre expresiones que ensalzan el terrorismo y aquellas que deben confluir en un espacio democrático y libre[23], el Tribunal Supremo considera que el enaltecimiento del terrorismo o la humillación de las victimas lo es cuando se haya llevado a cabo como "*una manifestación del discurso de odio*" o cuando provoquen "*una situación de riesgo para las personas o derechos de terceros o para el propio sistema de libertades*"[24].

Es evidente que el delito de enaltecimiento del terrorismo no supone una reducción ilegitima ni injustificada de los márgenes de la libertad de expresión, en tanto lo que se pretende evitar es estos actos apologéticos que producen perplejidad e indignación social y que, con esa base, son perseguidos por vía penal[25]. Más aún, la utilización de las redes sociales, incluso consultadas por menores de edad en etapas determinantes en el desarrollo humano, como el caso de la adolescencia, es caldo de cultivo para una radicalización sin control y la unión de nuevos adeptos a estas tendencias. Peor es la situación si se toma en cuenta que, muchas veces, la publicación de mensajes radicales y radicalizantes -que no necesariamente se mimetizan- se puede realizar solo con el fin de hacer bromas o una crítica social sin dimensionar la trascendencia que puede tener en otros. En estos casos, puede no ser delito de enaltecimiento y aun así producir el mismo efecto.

Siendo así, aunque es un delito penal de mera actividad y no de resultado, para muchos es inapropiado por sus consecuencias. Pero se debe considerar y sopesar la influencia persuasiva y represiva que supone la inclusión de un tipo penal como el considerado para intentar reducir la dañosidad de estos hechos, máxime con lo fácil que resulta consumir estos contenidos una vez son publicados y difundidos.

Es así como MIRÓ LLINARES, MONEVA & ESTEVE (2018: 2), tomando como referencia el caso específico de Twitter y los discursos ofensivos, consideran que esta y otras plataformas similares pueden constituir una especie de microambientes delictivos, en un sentido relacional porque "*la combinación de las personas (es decir, cuentas), que dicen cosas (es decir, tweets) a otras personas (es decir, otras cuentas), definen microambientes digitales únicos en el ciberespacio*", donde ocurren algunos delitos cibernéticos.

La solución más frecuente prevista para estos supuestos de enaltecimiento del terrorismo o humillación de las víctimas por vías tecnológicas ha sido la retirada de los contenidos. Pero su utilidad práctica se difumina por el hecho de que una vez subida una publicación a internet no puede recuperarse ni suprimirse con total eficacia o seguridad de todos los servidores a los que haya recibido acceso o las capturas de pantalla o fotos que pueden haberle registrado.

4. Los delitos informáticos terroristas

En el esquema aportado por el art. 573.2 CP, tal como se ha adelantado, se insertan como delitos terroristas determinados delitos informáticos cuando sean cometidos con alguna de las finalidades enumeradas en el mismo precepto. Supone una agravante específica de cada uno de los tipos de que se trate; a saber: los arts. 197 bis y 197 ter y 264 a 264 CP. Esto abarca conductas como las siguientes:

- El acceso o facilitación a otro del acceso a un sistema de información o mantenerse en el en contra de la voluntad de quien tenga derecho para excluirlo y vulnerando las medidas de seguridad establecidas.
- La intercepción de transmisiones no públicas de datos informáticos que se produzcan dentro de un sistema de información, utilizando artificios o instrumentos técnicos para conseguirlo.

[23] El Tribunal Constitucional ha reconocido que el derecho a la libertad ideológica no abarca solo una dimensión interna de la persona, sino también una externa con arreglo a las propias ideas sin sufrir sanción o desmérito o injerencia de los poderes públicos (STC 120/1990, FJ 10).

[24] Consúltese la STS 221/2017, de 29 de marzo, FJ 2.

[25] Así lo considera el Preámbulo de la Reforma del Código Penal introducida por la LO 7/2000.

- La producción, adquisición para su uso o importación de un programa informático o la contraseña de un ordenador, código de acceso o datos similares, sin estar debidamente autorizado y con el fin específico de cometer un delito con ellos.
- La supresión, daño, deterioro o la inaccesibilidad de datos o programas informáticos o documentos electrónicos ajenos, cuando el resultado producido haya sido grave. En este punto, se impone una pena superior si se realiza en el marco de una organización criminal o si se afecta una estructura crítica[26] o se hubiera creado una situación de riesgo.
- La obstaculización o interrupción grave y sin autorización en el funcionamiento de un sistema informático ajeno.

De esta manera, el dominio de la informática -que frecuentemente ha sido visto como elemento crucial para que materialicen sus objetivos- pasa a ser un claro escenario en el que los terroristas realizan los atentados. Por tal hecho, cuando se habla de ataques o actos terroristas no puede ya solo incluirse espacios físicos sino aquellos perpetrados *en* –que no *mediante*- ambientes digitales en los que se pueden afectar directamente infraestructuras esenciales para la sociedad y provocar temor a sus componentes, a través de una nueva y específica modalidad de violencia digital.

V. Áreas especialmente problemáticas en torno al terrorismo tecnológico

Siendo la red un amplísimo espacio en el que perpetrar crímenes terroristas, cabe destacar ciertos sectores en que la peligrosidad de que esto se produzca aumenta considerablemente. La finalidad de este apartado, por tanto, es la llamada de atención hacia estas páginas y plataformas virtuales, para así reforzar y perfeccionar la regulación que le es aplicable.

1. Las redes sociales

La táctica y la organización militar han variado poco a lo largo del tiempo, en comparación con las estrategias y esquemas comunicativos y propagandísticos que se hallan en continua evolución con las nuevas tendencias socio-tecnológicas. Internet permite una emisión directa del mensaje, por lo que favorece la difusión de actividades terroristas, fomentar el miedo por parte de estas organizaciones y reclutar adeptos (TAPIA ROJO, M.E; 2016: 373-375).

Hasta hace poco, *Twitter* era la red social por excelencia de los terroristas. Pero lo que buscan estos criminales son espacios con escaso control, por lo que, cuando la plataforma en línea refuerza sus canales de prevención y tratamiento del contenido terrorista, entonces deja de ser útil y atractiva para sus fines. Es lo que ocurrió con el mencionado servicio de microblogueo; Twitter empezó a ser más contundente a la hora de eliminar los contenidos y reduciendo la impunidad terrorista. La consecuencia de ello fue la migración de esta delincuencia a *Telegram*.

Consultando las Reglas y Políticas de Twitter, específicamente en la sección de "Política relativa a las organizaciones violentas" (*Safety and cybercrime*), se establece la nula tolerancia que da la plataforma a las organizaciones terroristas y a quienes se afilien a ellos o promuevan sus actividades ilícitas. Los análisis que realiza Twitter se fundamentan en las designaciones nacionales e internacionales sobre terrorismo, así como su propio criterio sobre los grupos extremistas y organizaciones violentas. Esto es lógico, considerando que no hay un concepto unívoco sobre terrorismo y, siendo que las redes sociales mueven masas en el mundo entero, es una necesidad que abarque las distintas concepciones de dicho fenómeno a escala global.

En virtud de ello, se establece que las siguientes conductas infringen el código de uso de la red social:

- La comisión o promoción de actos en nombre de una organización violenta.

[26] La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, define estas como "*las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*" de la sociedad. Y a e escala europea, son aquellas infraestructuras "*situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros*" (art. 2).

- El reclutamiento de miembros para una organización violenta.
- La distribución de servicios para el beneficio de los objetivos de una organización violenta.
- El uso de la insignia o los símbolos de organizaciones violentas para su promoción o para ser indicativo de afiliación o apoyo.

En caso de incumplimiento de la política de Twitter –que puede ser objeto de denuncia por cualquier persona, independientemente de si tiene cuenta en la plataforma o no-, la consecuencia es la suspensión de cualquier cuenta de "*forma inmediata y permanente*". Por eso, aunque Twitter sigue siendo una herramienta para la difusión del mensaje terrorista, la presencia de estos perfiles está siendo bastante controlada y limitada por lo que los terroristas han experimentado en otras redes sociales menos conocidas.

Esto fue así hasta la creación de Telegram en 2013. Son tres los servicios esenciales ofrecidos por la plataforma que resulta de especial atractivo para los terroristas: su "revolucionaria" política de privacidad; la limitación que tiene a la hora de procesar solicitudes de terceros para quitar contenidos y; los chats secretos:

a. La política de privacidad: Dentro de las FAQs que se encuentran en la página oficial de la plataforma y que responden a dudas básicas sobre Telegram, se expone que "*el objetivo de Telegram es crear un servicio de mensajería verdaderamente libre, con una política de privacidad revolucionaria*". Entre otras cosas, esto se logra –dice también el documento- protegiendo las conversaciones privadas de terceras partes curiosas como, por ejemplo, funcionarios.
b. El limitado procesamiento de solicitudes de terceros para retirar contenido: Establece también Telegram que "*todos los chats y grupos* […] *son territorio privado de sus respectivos participantes y no procesamos solicitudes relacionadas a ellos*". Aunque se específica que bloquean *bots* y canales terroristas, no serán bloqueados quienes expresan pacíficamente opiniones alternativas. No obstante, esto tendrá lugar solo cuando se trate de contenido público ilegal en Telegram, es decir, sets de stickers, *bots* y canales.
c. Los chats y grupos secretos*:* Aunque los canales estén prohibidos, Telegram sigue siendo un buen puente para los terroristas. La posibilidad de adquirir tarjetas SIM y el cifrado de los mensajes dificulta la identificación del autor de la difusión del contenido ilícito. Y es que los chats secretos usan cifrado *end-to-end*, por lo que Telegram no tiene datos que puedan relevarse. Además, su estructura y diseño están pensados para evitar la cesión de datos a los organismos jurisdiccionales. Los datos de los chats en la nube se almacenan en centros de datos alrededor del mundo y nunca se mantienen en el mismo lugar, por lo que "*varias órdenes judiciales de diferentes jurisdicciones son requeridas para forzarnos* -a la plataforma, según lo expresado en sus FAQs- *a entregar algún dato*". Además, las claves de cifrado relevantes son divididas en partes y no se mantienen en ningún momento en el mismo lugar que los datos protegidos.

También hay grupos secretos que, en contraste con los públicos -que llevan un alias disponible desde el buscador o desde el URL acortado y cuyos mensajes pueden ser previsualizados por cualquier usuario antes de unirse-, tienen un enlace de invitación cambiable y cuyo contenido no puede ser visto hasta que el invitado sea aceptado. Este método, sin duda, no es lo suficientemente contundente como para frenar la difusión y acceso a estos grupos que, como se ha visto, podrían manejar contenido que no podrá ser objeto de control por la política de privacidad de Telegram.

En realidad, las plataformas de redes sociales se encuentran en una situación complicada, ya que la apuesta por medidas como las mencionadas pretende la protección de la privacidad de los usuarios en general, no favorecer a los terroristas. Pero la capacidad de adaptación de estos últimos las convierten en riesgos. Los casos de Twitter y Telegram ejemplifican el comportamiento de los terroristas en redes sociales. Acuden a ellas por el alcance y repercusión que consiguen con ellas de forma directa e instantánea y, muchas veces, poco limitada. No obstante, su permanencia en ellas dependerá de la forma en que la plataforma responda a la lucha antiterrorista. A medida que el control de los contenidos y las sanciones consecuentes se hagan más robustos, los ciberterroristas buscarán otras alternativas. Esto permite ver desde ya una idea importante: el comportamiento de las plataformas de redes sociales puede tener mucha transcendencia a la hora de evitar el terrorismo en Internet.

2. La Dark Web

Aunque los peligros de la *dark web* no se circunscriben solo al terrorismo, esta área delictiva halla en dicho sector de la web un excelente sitio para perpetrar sus actos criminales y alcanzar sus fines ilícitos. La razón de esto es que para acceder a la llamada "Internet oscura" -que representa alrededor del 6% del Internet total- se requieren de herramientas y navegadores específicos. Por eso resulta el contenedor ideal para contenidos ilegales.

Las organizaciones terroristas y, por extensión, sus adeptos, han incrementado el uso de la *dark web* por sus condiciones de seguridad y el elevado volumen de recursos que ofrece. Entre estos, en la Internet profunda hay disponibles salas de chat o foros que se benefician del anonimato que proporciona TOR[27], con una estructura y jerarquía similar a los foros tradicionales disponibles en la *surface web* (Yuste, C.; 2015: 17 y 18). De esta manera, esta porción de la red mundial se ha convertido en una poderosa herramienta para que las organizaciones terroristas difundan propaganda, recluten nuevos miembros y financien y planifiquen sus actividades. El anonimato y la clandestinidad que ofrece la *dark web* resulta particularmente peligrosa en este sentido. Pero el riesgo va más allá. Y es que el acceso a la misma no es ilegal; solo lo es el contenido que se puede adquirir en ella. Ni tampoco es especialmente complicado entrar en estos sitios.

Conscientes de lo expuesto, los servicios y unidades de Inteligencia han dedicado muchos esfuerzos para contrarrestar las actuaciones de, entre otros que delinquen en la *dark web*, los terroristas. Uno de ellos han sido los proyectos *DANTE* y *Trivalent*, financiados ambos por la Comisión Europea y ejemplos de la inclusión de la Inteligencia Artificial como recurso de apoyo en la lucha criminal. En ambos se utiliza, entre otras cosas, la tecnología desarrollada por *Expert System*, la cual -con análisis de texto contextualizado- permite detectar terminología yihadista, localizar adoctrinados, descubir información engañosa y perfiles comunes en redes sociales. Con estos datos, los cuerpos de seguridad pueden identificar a los terroristas adoctrinados.

Específicamente DANTE no se limita solo al análisis de textos y recopilación de datos o archivos, sino que también descubre mensajes codificados; identifica y agrupa las actividades y eventos que pueden estar organizando los terroristas; reconoce falsificaciones y manipulaciones al identificar diseños y personas; distingue idiomas y detecta los hablantes y sonidos a partir de archivos de audio y; por si fuera poco, identifica campañas de recaudación de fondos para el terrorismo en Internet, detectando transacciones financieras inusuales e identificando a los autores o sospechosos por su identidad digital. Dicho proyecto ha sido un éxito y una herramienta constante por numerosos funcionarios que le han dado uso y alcanzado buenos resultados en la investigación de los crímenes terroristas en la web.

La lección que se extrae de lo expuesto es que las ventajas que ofrece el mundo virtual para la perpetración de actos de esta índole son tantas que el Derecho suele tener un ritmo más aletargado para darle respuesta. No quiere decir que todo este perdido en la batalla contra el terrorismo cibernético, si la represión penal y policial de estos hechos se combina con novedosas herramientas informáticas que agilicen la detección y tratamiento del ciberterrorismo. Los proyectos mencionados son ejemplo de eso: la interacción de la ciencia jurídica y la tecnología se hace cada vez más necesaria. La experiencia ha demostrado que el Derecho, por sí solo, no puede dar una respuesta eficaz al vertiginoso avance de las tecnologías y contrarrestar el uso ilícito de las mismas, especialmente en el caso del terrorismo[28].

---

[27] El Navegador TOR ('*The Onion Router*') es el proyecto dedicado a crear una red de comunicaciones distribuida y superpuesta a Internet. Tor implementa la técnica *Onion Routing* para proteger las comunicaciones, garantizar el anonimato y la privacidad de los datos[27]. Este navegador web de código abierto surgió como medio de protección de los usuarios de internet que quedaban expuestos a ataques de vigilancia. Entre sus funciones se encuentran: la encriptación compleja de datos antes de ser enviados por internet, desencriptación automática de datos en el lado del cliente, la anonimidad total sin importar el servidor o la página web, el permiso para visitar páginas bloqueadas en nuestra región, la realización de tareas sin revelar la IP verdadera del usuario, el envío de datos desde y hasta servicios escondidos y aplicaciones detrás de cortafuegos, así como la recepción segura de archivos de terceros.

[28] En este sentido, GÓNZALEZ NAVARRO insiste en que "*debido a que las tecnologías de la comunicación han evolucionado y en la actualidad el proceso comunicativo tiene lugar a través de estas vías*, [parece lógico que] *se proceda también a la incorporación de las nuevas tecnologías como medios de investigación del delito*". En Terrorismo, sistema penal y derechos fundamentales. Alberto Alonso Rimo, María Luisa Cuerda & vv.aa (dir), 2018. También *vid*. MORÁN BLANCO, S. En REDI, Vol. 68, 2017; quien destaca que los Estados están en la obligación de articular un sistema nacional de ciberseguridad, que proporcione un uso seguro de las TICs y, en general, del ciberespacio. En relación con esto y, en torno al

3. Las monedas virtuales

En noticias recientes se ha destacado el alto nivel de ingresos que, en la actualidad, reciben las organizaciones terroristas en forma de criptomonedas. Hay fuentes que han advertido que los terroristas de *ISIS, Al Qaeda y Hamas* recaudan más de mil millones de dólares anuales en criptomonedas, es decir, a través de transacciones con divisas virtuales[29]. Por ejemplo, en 2020 la policía francesa, gracias a una operación encubierta, detectó una red que financiaba el terrorismo comprando cupones de criptomonedas de entre 12 y 176 dólares en puntos de venta de tabaco en Francia, los cuales eran utilizados para acreditar las cuentas de *Bitcoin* de sus cómplices en Siria.

Esta realidad ha obligado a las autoridades y agencias de seguridad a gestionar y destinar recursos en pos de regular debidamente el uso de las criptomonedas, por el alto riesgo de que sean utilizadas para actividades ilegales. Así lo manifiesta el caso de EEUU que diseña una ley que permite la investigación del mercado de las monedas criptográficas para determinar su utilización en el caso del terrorismo. Incluso, curiosamente, se ha noticiado que el Departamento de Estado ofrece hasta 10 millones de dólares en criptomonedas a cambio de información sobre terroristas y extremistas a través de una plataforma segura que algunos consideran como el precursor de iniciativas similares de *ciberpolicía.*

El auge de las criptomonedas está cambiando el mundo, ya no solo en términos financieros, sino en el desarrollo de comportamientos delictivos y la estructura de control que se erige frente a ellos. Eso obliga a la ciencia jurídica, específicamente el Derecho penal, a mantenerse al tanto de las novedades y particularidades en este sector, para así contrarrestar sus efectos, pero sin que las tecnologías criptográficas -que mueven una cantidad importante de dinero- pierdan sus funcionalidades y beneficios. La solución no debería ser la de demonizar un avance tecnológico tan útil, sino establecer límites y regulaciones claras y proporcionales para enmarcarlo en un halo garantista y seguro.

Esto es especialmente importante, hoy día, en el caso de las divisas virtuales. Aunque su vertiginosa aparición en la escena pública es de data reciente, no es una justificación para mantener por más tiempo un escaso y difuso control sobre aquellas. El anonimato que ofrecen y el escaso control por parte de los entes públicos son algunas de las características que convierten a estos monederos digitales como elemento clave en la comisión de hechos delictivos.

No obstante, es necesario aclarar que el mayor uso que se le da a las criptomonedas es para fines legítimos, por lo que su utilización indebida tiene cierto carácter residual. Pero esa pequeña porción de casos en que facilitan la perpetración de crímenes es bastante riesgosa. Por tanto, es perentoria la necesidad de una nueva y perfeccionada legislación en torno a esta área; una regulación orientada a la detección de los supuestos delictivos y no a una prohibición o inutilización -directa o indirecta- de las criptomonedas[30].

4. El Metaverso

El ecosistema metavérsico, inspirado en juegos muy famosos, se ha convertido en un espacio virtual colectivo y convergente con la realidad física. Su funcionamiento parte de tecnologías de realidad virtual, aumentada y mixta y, partiendo de ellas, ofrece grandes posibilidades en torno a la socialización. Ha configurado un mundo de posibilidades, donde las personas realizan actividades tan cotidianas como

terrorismo concretamente, la autora, muy acertadamente, reflexiona sobre la carencia de instrumentos universales específicamente dedicados al ámbito del ciberterrorismo, dejando abierto el debate sobre su pertinencia y necesidad.

[29] Véase, por ejemplo, el informe titulado: "*Los terroristas de ISIS, Al Qaeda y Hamas recaudan más de 1.000 millones de dólares al año en criptomonedas*". Disponible en Infobae a través del siguiente enlace: https://www.infobae.com/america/mundo/2021/06/27/los-terroristas-de-isis-al-qaeda-y-hamas-recaudan-mas-de-1000-millones-de-dolares-al-ano-en-criptomonedas/.

[30] *Vid.* GONZÁLEZ CUSSAC, J.L. Tecnocrimen. En Nuevas amenazas a la Seguridad Nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación. Gónzalez Cussac, J / Cuerda Arnau, M.L. (dir.); Fernández Hernández, A. (coord.), Editorial Tirant Lo Blanch, 2013. El autor remarca que la armonización legislativa a nivel mundial sobre lo que llama "*tecnocrimen*" permitiría "*salvar el obstáculo de las fronteras y poder investigar, capturar y enjuiciar a los atacantes en cualquier lugar del mundo donde se encuentren -incluso si utilizan servidores Proxy-, ya que sería más sencillo ubicarlos*".

interactuar con otros, jugar, trabajar, educarse, entre otras[31].

De esta forma, el Metaverso supone un nuevo paradigma de las interrelaciones sociales e interesa atender jurídicamente lo que está ocurriendo allí[32]. Las tecnologías hapticas permiten sentir realmente lo que se experimenta en el *e*-universo e. incluso, grandes empresas están ya diseñando *gadgets* que permiten sentir dolor. Naturalmente, conductas delictivas clásicamente previstas para el contacto físico y la realidad material adquieren una nueva concepción al tratarse de un ecosistema digital como este. En virtud de ello, se han destacado diversos retos que afronta -o se prevé que afrontará- el Derecho frente al Metaverso.

A efectos de este trabajo, ante la avanzada inmersión digital, se ha advertido que las organizaciones terroristas pueden valerse del universo digital para reclutar y captar adeptos, coordinar y planificar ataques o bien, perpetrarlos en el propio entorno virtual. Lo primero es fácil de imaginar, pues las facilidades que ofrece el Metaverso para forjar comunicaciones ideológicas y sociales es evidente. Pero quizás es más difícil de admitir la repercusión que tendría un ataque *en* el propio espacio digital.

No obstante, recrear ataques terroristas en el Metaverso puede ser una experiencia con daños perceptibles a nivel psicológico y que fomente el miedo en la población digital. De momento, lo más lógico y coherente con el principio de *ultima ratio* y proporcionalidad que caracteriza al Derecho penal parece ser considerar que son comportamientos desdeñables e innecesarios, pero que no son reales por lo que no constituyen un ilícito que merezca el reproche penal que recibe el terrorismo. Ahora bien, si el Metaverso realmente se convierte en el futuro de la convivencia humana y este tipo de conductas amedrentadoras se hacen frecuentes, la posición frente a ellas puede ser diferente y más contundente, si se mide que los daños son efectivamente reales. Pero para eso hace falta tiempo e investigación.

Como se infiere de la anterior reflexión, aún no es posible -por su auge reciente- ser categóricos en lo que al Metaverso se refiere. Pero sí es un área que merece atención desde ahora, para que la interacción inmersiva sea segura y coherente con las exigencias jurídicas y así, no cometer los mismos errores que en el mundo físico.

VI. Expectativas y propuestas para la lucha contra el (ciber) terrorismo

Como se hace patente a lo largo de la presente investigación, la tecnología ha pasado de ser solo un medio para cometer crímenes a tener entidad propia y configurar un fin en sí mismo. Esto es especialmente interesante en al campo del terrorismo donde su modalidad virtual constituye delitos autónomos y complejos que muchas veces pasan desapercibidos y se solapan en el terrorismo tradicional.

El ciberterrorismo debe ser objeto de atención particularizada. Las aulas universitarias y centros de enseñanza donde se imparten conocimientos criminológicos y jurídicos deben incidir en la utilización de medios informáticos por parte de los terroristas y fomentar el interés por desarrollar nuevas líneas de investigación en este campo. Los docentes y profesionales deben destacar la idea de que financiar el terrorismo con criptomonedas, por ejemplo, no es una vía para perpetrar un atentado; sino que es un delito autónomo y peligroso *per se*. Que la atención se focalice individualmente en cada delito y no verlos como un *puzzle* -aunque todos conforman el fenómeno terrorista- puede ser un método eficaz a la hora de lucha contra dicha amenaza social.

El resultado de dicha atención será el diseño de mecanismos legales e informáticos que favorezcan la detección y faciliten la respuesta que se brinde a estos casos. En relación con los primeros, la regulación jurídico-penal debe perfeccionarse, sobre todo en lo que respecta a la organización de los delitos y su ubicación

[31] Varios informes y estadísticas recientes permiten notar la situación del Metaverso en España. Por ejemplo, según el estudio titulado "*How the World sees the Metaverse and extended reality*", realizado por *Ipsos* en colaboración con el Foro Económico Mundial, España es muy favorable y optimista con el potencial que ofrece la tecnología inmersiva. De hecho, es el país más familiarizado de Europa con estas innovaciones digitales, situándose 9 puntos por encima de la media global. Asimismo, en la última edición del estudio sobre redes sociales de *IAB Spain* se reflejó que casi 1 de cada 10 españoles ya está en el Metaverso.

[32] *Vid*. SERRANO ACITORES, A. Metaverso y Derecho. Editorial Tecnos. También, TRALLERO MASÓ, A. & TOMÁS ROMÁN, E. Metaverso y Derecho Penal. En La Ley Penal, Nº 158, 2022.

sistemática. La técnica más empleada en el Código Penal para tipificar los delitos ciberterroristas es insertarlos como un apartado más dentro de las modalidades tradicionales. Eso puede conllevar una visión más difusa del terrorismo tecnológico, ya que se solapa entre otras figuras delictivas.

En relación con los mecanismos informáticos, la incorporación de sistemas tecnológicos es lo ideal si se quiere una identificación y tratamiento eficaz del terrorismo digital. El mundo virtual, como se ha destacado, es un nuevo escenario para la comisión de delitos, lo que hace necesario que los mecanismos de control también formen parte de ese mismo mundo. Será prácticamente imposible responder a hechos digitales con instrumentos meramente materiales. En ese sentido, resultarán de gran utilidad programas de Inteligencia Artificial (IA) y técnicas de *Bigdata* para filtrar y procesar datos en la red.

Ahondando en lo anterior, también resulta pertinente el análisis de la responsabilidad de los servidores de plataformas web a la hora de minimizar los daños ocasionados por el terrorismo tecnológico. Siendo las redes sociales un campo muy usado por los terroristas para difundir su mensaje y conseguir adeptos y sin dejar de garantizar la privacidad de los usuarios, estas plataformas deben garantizar un alto nivel de seguridad en torno a este peligro, pero sin poner en riesgo la privacidad general de los usuarios, lo que produce una encrucijada en muchos casos. Además, conscientes del alcance instantáneo que tienen los *posts* que se realizan en ellas, la eliminación de contenido en caso de constituir delitos o información socialmente reprobable no basta. Una vez que una publicación ha sido subida a Internet ya es imposible canalizar -ni siquiera calcular- los daños que puede causar[33].

Por otra parte, se debe incidir en la pauta fijada por la Estrategia Nacional contra el Terrorismo de 2019. Dentro de las líneas estratégicas planteadas se estableció, entre otras cosas, lo siguiente: "*promover campañas en Internet y redes sociales que hagan frente al discurso extremista violento, colaborando e implicando especialmente a la sociedad civil y al colectivo de jóvenes*"[34]. Y en coherencia con lo previo, se recomienda *impedir* –no eliminar *a posteriori*- el alojamiento de contenidos y canales idóneos para el adoctrinamiento, reclutamiento o la difusión de ideales terroristas.

No obstante lo expuesto y a pesar de lo dañino que resulta el terrorismo, nunca se debe perder de vista el importante principio de proporcionalidad y, sobre todo, el derecho a la privacidad y a la libertad de expresión que tienen *todas* las personas. Por tanto, no es una batalla sencilla ni está todo dicho, por lo que todo debate e investigación que se realice en relación con el ciberterrorismo será un aporte muy agradecido.

[33] Por ello, iniciativas como la de la Universidad de Vigo para detectar contenidos terroristas con IA *antes* de hacerse públicos puede ser una consideración interesante. Y es que, un grupo de investigadores de este Centro participan en un proyecto europeo, que pretende el desarrollo de una herramienta al servicio de las Fuerzas y Cuerpos de Seguridad, para la detección de comunicaciones escondidas terroristas en contenidos, mediante la utilización de la IA. También merece ser destacado el Proyecto CT-Tech (2022-2024), relativo a la utilización de las tecnologías nuevas y emergentes en la lucha contra el terrorismo. Esta iniciativa parte de la idea de que la INTERPOL debe atender las nuevas terroristas en un doble sentido: para entender cómo son utilizadas por tal sector criminal y cómo pueden usarlo los Estados y sus autoridades para anticiparse a los problemas que conciernen las ciberactividades terroristas.

[34] En España, la cultura de defensa es la idea iniciativa de construir un sistema de seguridad en la lucha contra la ciberdelincuencia con la colaboración de la ciudadanía. El Ministerio de Defensa promueve la inclusión de una cultura de defensa para conseguir el apoyo de la sociedad y para lograr la verdadera y genuina defensa por la ciudadanía en general. Una política de promoción de una cultura de defensa involucra la actuación de los poderes públicos, de las organizaciones y actores de la sociedad civil.

Bibliografía

ANDRADE, O.D. (2015). Terrorismo: entre la política y la criminalidad. Revista Análisis Internacional, 6 (2), 67-82.

ASUA BATARRITA, A. (2002). Concepto jurídico de terrorismo y elementos subjetivos de finalidad. Fines políticos últimos y fines de terror instrumental. En J.I. Echano Basaldua y J.M. Lidón Corbi (coords.). Estudios jurídicos en memoria de José María Lidón. Bilbao: Deustuko Unibertsitatea, Servicio de Publicaciones = Argitalpen Zerbitzua.

ASUA BATARRITA, A. (2006). El discurso del enemigo y su infiltración en el Derecho penal. Delitos de terrorismo, "finalidades terroristas" y conductas periféricas. En M. Cancio Meliá y Gómez-Jara (coords.). Derecho penal del enemigo. El discurso penal de la exclusión. España: Editoriales Edisofer.

AZNAR, J. (2016). Los Delitos de Terrorismo (Arts. 571 a 580 del Código Penal). Universidad de Zaragoza.

BAYARRI GARCÍA, C.E. (2018). Los nuevos delitos de terrorismo. Adoctrinamiento activo y pasivo vs. enaltecimiento y provocación a la comisión de delitos terroristas. En A. Alonso Rima y M.L. Cuerda (dir.). Terrorismo, sistema penal y derechos fundamentales. España: Tirant Lo Blanch.

CANCIO MELIÁ, M. (2010). Los delitos de terrorismo: estructura típica e injusto. Madrid: Editorial Reus.

CANCIO MELIÁ, M. (2018). El concepto jurídico-penal del terrorismo entre la negación y la resignación. En A. Alonso Rima y M.L. Cuerda (dir.). Terrorismo, sistema penal y derechos fundamentales. España: Tirant Lo Blanch.

CANO PAÑOS, M.A. (2019). La violencia terrorista como espectáculo en internet: una aproximación criminológica. Revista Científica General José María Córdova, Vol. 17, 28, 691-717.

DOMINGO, C. (2018). Bitcoin, criptomonedas y Blockchain. España: Editorial Planeta.

FERNÁNDEZ HERNÁNDEZ, A. (2013). Ciberamenazas a la Seguridad Nacional. En J. González Cussac y M.L. Cuerda Arnau (dir.). Nuevas amenazas a la Seguridad Nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación. Gónzalez Cussac, J / Cuerda Arnau, M.L. (dir.); Fernández Hernández, A. (coord.). Valencia: Editorial Tirant Lo Blanch.

FRANCISCO AGRA, S. (2021). Una aproximación al (ciber) terrorismo: Modelos previos y actuales. DOCRIM: Revista Científica, 8.

GAMÓN, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20.

GARRIDO, Á. (2015). Los delitos de terrorismo en el Código Penal Español. La nueva regulación introducida por la Ley Orgánica 2/2015. Universidad de Zaragoza.

GONZÁLEZ, L. (1997). Las nuevas tecnologías de comunicación como una nueva expresión de las ideologías de exclusión: el caso del sistema educativo mexicano a nivel superior. Relieve, 16, 2.

GONZÁLEZ NAVARRO, A. (2018). El uso de nuevas tecnologías en la investigación de delitos de terrorismo. En A. Alonso Rima y M.L. Cuerda (dir.). Terrorismo, sistema penal y derechos fundamentales. España: Tirant Lo Blanch.

JAKOBS, G. / CANCIO MELIÁ, M. (2003). Derecho Penal del Enemigo. Madrid: Thomson Civitas, Cuadernos Civitas.

LAMARCA PÉREZ, C. (1985). Tratamiento jurídico del terrorismo. Ministerio de Justicia, Secretaría General Técnica.

LAMARCA PÉREZ, C. & MIRA BENAVENT, J. (2013). Noción de terrorismo y clases. Evolución legislativa y político-criminal. En C. Fernández- Pacheco y C. Juanatey Dorado (dir). El nuevo panorama del terrorismo en España: perspectiva penal, penitenciaria y social. Alicante: Servicio de Publicaciones de la Universidad de Alicante.

LAMARCA PÉREZ, C. (2019). Tema 25. Delitos contra el orden público. En C. Lamarca Pérez, A. Alonso de Escamilla y vv.aa (coord.). Delitos. La parte especial del Derecho Penal. España: Editorial Dykinson.

LLOBET ANGLÍ, M. (2015). ¿Terrorismo o terrorismos?: Sujetos peligrosos, malvados y enemigos. Revista Jurídica, 31, Universidad Autónoma de Madrid.

LLOBET ANGLÍ, M. (2015). Lobos solitarios yihadistas: ¿terroristas, asesinos o creyentes? Retorno a un Derecho penal de autor. En S. Alda Mejías, G. Colom y vv.aa. Actas VII Jornadas de Estudios de Seguridad, Colección de Investigación, Instituto Universitario General Gutiérrez Mellado.

LÓPEZ CALERA, N. (2002). El concepto de terrorismo ¿Qué terrorismo? ¿Por qué el terrorismo?. ¿Hasta cuándo el terrorismo? Anuario de Filosofía del Ferecho, 19.

MARTÍN, M.A. (2020). El Estado Islámico, un universo semiótico: análisis de la revista Dabiq. Universidad Complutense de Madrid.

MEMBIELA, M.E. & PEDREIRA, N. (2019). Herramientas de Marketing digital y competencia: una aproximación al estado de la cuestión. Atlantic Review of Economics, 3, 3.

MIRÓ LLINARES, F. (2015.) La criminalización de conductas "ofensivas". A propósito del debate anglosajón sobre los "límites morales" del Derecho penal. Revista Electrónica de Ciencia Penal y Criminología, 17.

MIRÓ LLINARES, F.; MONEVA, A. & ESTEVE, M. (2018) Hate is in the air! But where? Introducing an algorithm to detect hate speech in digital microenvironments. Crime Science, 7.

MORENO, J.D. (2017). Análisis del nuevo delito de autoadoctrinamiento del artículo 575.2 del Código Penal incorporado con la Ley Orgánica 2/2015. Anuario de derecho penal y ciencias penales, 70, Mes 1.

OLMEDO, M. (2015). Capítulo 71. Delitos contra el orden público (VI). De las organizaciones y grupos terroristas. Delitos de terrorismo. En L. Morillas Cueva (coord.). Sistema de derecho penal: Parte especial (2a Edición).

PARRONDO, L. (2018). Tecnología Blockchain, una nueva era para la empresa. Revista de Contabilidad y Dirección, 27, 11-31.

PASTRANA, M.A. (2020). La nueva configuración de los delitos de terrorismo. Imprenta Nacional de la Agencia Estatal. Boletín Oficial del Estado.

PÉREZ, A. (2020). Ciberterrorismo, ¿una nueva amenaza? Instituto Español de Estudios Estratégicos, 106.

PÉREZ, D. (2020). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. Boletín Criminológico, Encuentro de Jóvenes Investigadores en Criminología, 206.

POLAINO-ORTS, M. (2009). Derecho Penal del Enemigo. Fundamentos, potencial de sentido y límites de vigencia. Barcelona: Editorial Bosch, 1ª Edición.

RANGEL, L. (2019). Aproximaciones jurídicas al marco regulatorio de las criptomonedas. Caracas: Luis José Rangel Gutiérrez Editores.

RODRÍGUEZ, J.A. (2004). La red terrorista del 11M. REIS: Revista Española de Investigaciones Sociológicas, 107.

SÁNCHEZ-GIL, L. (2021). Repensando el concepto de ciberterrorismo. Instituto Español de Estudios Estratégicos, 11.

SÁNCHEZ MEDERO, G. (2010). La nueva estrategia comunicativa de los grupos terroristas. Revista Enfoques, Vol. 8, 12, 201-215.

SERRANO ACITORES, A. (2022). Metaverso y Derecho. Madrid: Editorial Tecnos.

SOMIEDO, J.P. (2015). La estructura y la organización de los grupos terroristas bajo la óptica del aprendizaje organizacional. Instituto Español de Estudios Estratégicos, 24, 2015.

TAPIA ROJO, M.E. (2016). Análisis de la estrategia comunicativa del terrorismo yihadista. El papel de las redes sociales. Instituto Español de Estudios Estratégicos, 1.

TRALLERO MASÓ, A. & TOMÁS ROMÁN, E. (2022). Metaverso y Derecho Penal. La Ley Penal, Nº 158.

TORRES SORIANO, M. (2007). La dimensión propagandística del terrorismo yihadista global. Universidad de Granada.

UNODC. (2013). El uso de internet con fines terroristas. Nueva York: Naciones Unidas. Recuperado de:

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf.

YUSTE, C. (2015). Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas. Universidad Internacional de la Rioja.