CENTRO DE INVESTIGAÇÃO
INTERDISCIPLINAR
EM JUSTIÇA

CIJ Research Papers
Cadernos de Investigação CIJ

5 | 2024

PERSPECTIVAS Y DESAFÍOS DEL TERRORISMO EN LA ERA DIGITAL ATENDIENDO AL DESPLAZAMIENTO PARADIGMÁTICO DE LAS MODALIDADES TRADICIONALES

Samar Francisco Agra

Departamento de Derecho Penal de la Universidad de Granada

Ficha Técnica

Autor | Samar Francisco Agra
Título | Perspectivas y Desafíos del Terrorismo en la Era Digital Atendiendo al Desplazamiento Paradigmático de las Modalidades Tradicionales
Data de Publicação| Setembro 2024
ISSN | 2975-836X
DOI | 10.34626/2975-836x/2024_5

Edição

Centro de Investigação Interdisciplinar em Justiça (CIJ) / Centre for Interdisciplinary Research on Justice (CIJ)
Financiamento | Este trabalho foi desenvolvido com o apoio da Fundação para a Ciência e a Tecnologia (FCT) – UIDB/00443/2020 (Centro de Investigação Interdisciplinar em Justiça)

Comissão Editorial

Secretariado

Contactos

Telefone | 222 041 610
Email | cij@direito.up.pt
Morada | Faculdade de Direito da Universidade do Porto
Rua dos Bragas, 223
4050-123, Porto
Portugal

PERSPECTIVAS Y DESAFÍOS DEL TERRORISMO EN LA ERA DIGITAL ATENDIENDO AL DESPLAZAMIENTO PARADIGMÁTICO DE LAS MODALIDADES TRADICIONALES

Samar Francisco Agra

Departamento de Derecho Penal de la Universidad de Granada

(Quaisquer questões relacionadas com o conteúdo do presente artigo deverão ser dirigidas ao autor, através do seguinte endereço de email: samarfr@ugr.es)

Resumen

El terrorismo es un fenómeno flexible que se va adaptando en función de las realidades que emergen y de las herramientas que están a su alcance. Ante esto, el desarrollo de nuevas tecnologias ha supuesto un factor transformador del terrorismo conocido antes de la era digital, no solo en sus manifestaciones materiales sino en las implicaciones emocionales tan complejas que motivan a sus autores. En este trabajo se abordan estas cuestiones, mirando el fenómeno de forma retrospectiva y, a partir de allí, analizando las realidades actuales y las posibilidades futuras. Con especial rigor, se considerarán determinadas áreas tecnológicas susceptibles de ser utilizadas en el ámbito terrorista, dado su marcado interés a nivel fenomenológico y de ciberseguridad.

Abstract

Terrorism is a flexible phenomenon that adapts according to the realities that emerge and the tools that are available to it. Thus, the development of new technologies has been a transforming factor in the terrorism known before the digital era, not only in its material manifestations but also in the complex emotional implications that motivate its perpetrators. This paper addresses these issues, looking at the phenomenon retrospectively and, from there, analysing current realities and future possibilities. Particularly rigorous consideration will be given to certain technological areas likely to be used in the field of terrorism, given their strong phenomenological and cyber-security interest.

Índice

Introducción

El terrorismo no es solo un delito, es más que eso. Es una de las mayores amenazas para la paz y la seguridad internacionales y, peor aún, es uno de los actos que más violenta los derechos humanos y las libertades fundamentales de las personas. Ciertamente, es un fenómeno imprevisible y, ante lo imprevisible lo único que puede hacerse es hacer todo lo que esté al alcance para emplear medidas preventivas. Una forma de hacerlo es analizando la realidad fenomenológica acontecida hasta ahora, para establecer patrones y definir factores de cambio. Así, remontarnos al pasado histórico de un hecho tan trascendental y dañoso como el terrorismo es una forma de afrontar el presente y el futuro con las lecciones mejor aprendidas. Y no porque siempre se proyecte de la misma manera, sino porque hay patrones comunes. Este punto de partida puede facilitar mucha información a la hora de desarrollar las políticas y los programas antiterroristas, aunque enmarcándolos en las distintas formas en que se ejecutan estos hechos delictivos, pues cada una de ellas requerirá distintos medios y regulaciones para su eficaz represión y, sobre todo, prevención.

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; entre otras cosas, de la mano del crecimiento vertiginoso de instrumentos y estructuras digitales. De esta forma, el terrorismo ha ido consolidándose aún más como un crimen transnacional, amenazante y permanente. Esto ha exigido un Derecho penal que enmarque un proceso de justicia eficiente y legítimo. Una respuesta eficaz ya no se proyecta solo en castigar los delitos terroristas, sino en comprender el funcionamiento de escenarios previos. 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.

1. Condicionantes Conceptuales Y Descriptivos

1.1. Propuestas definitorias

Previo a la descripción e identificación de las implicaciones de cualquier fenómeno, la ciencia intenta proporcionar una definición o concepto como aproximación inicial. La ciencia jurídica no es la excepción. No obstante, no siempre es sencillo ni, por más esfuerzos que se lleven a cabo, posible, que el Derecho siempre pueda sostener un concepto unívoco y homogéneo. Ésta disciplina científica se caracteriza por la interpretación, integración y sistematización de las normas; caracterizadas ellas por su necesaria formalidad. Pero el Ordenamiento jurídico debe analizar y aplicar los preceptos que le conforman de acuerdo con el entorno social en que rija.

El problema es que el alcance del terrorismo, tanto en sentido material como en sentido territorial, desdibuja la posibilidad de forjar un concepto absoluto. De hecho, la mayoría de los que se han ofrecido, parecen acercarse más a una descripción que a una definición en sí misma. Esto obedece a la intención de abarcar todos los extremos posibles de este fenómeno, en aras de mejorar su regulación jurídica a posteriori. Más aún, se tiene el deseo de que dicha regulación traspase fronteras -así como también las ha traspasado el terrorismo-, para lo cual se ha sostenido la necesidad de un concepto universal como germen de una cooperación internacional más clara.

Sin embargo, una cooperación efectiva no ha de depender de un concepto jurídico único, aunque es un importante basamento, sino en diseñar recursos eficientes y solidarios en los distintos estamentos; no solo a nivel macro, como en el seno de la ONU o la UE, sino a un nivel más micro, como las entidades regionales y/o locales. No quiere decir esto que definir tal concepto sea minucia, sino que, probablemente, cada Estado incluirá en su regulación aquellos aspectos del terrorismo que sean prioridad en su territorio (Rodríguez Morales, T., 2012: 77). Quizás, construir un concepto internacional sería contraproducente, en la medida en que limitaría la regulación en cada lugar y no la personalizaría de acuerdo a sus necesidades.

Pero hay otro aspecto que se ha de destacar. En realidad, el término "terrorismo" no es un concepto absolutamente adscrito al mundo jurídico, aunque sea un importante foco de atención de esta ciencia y constituir aquel un acto –o serie de ellos- con serias repercusiones penales. Naturalmente, definir un concepto multidisciplinar es un reto con un plus de dificultad[1], más aún si es una construcción necesariamente envuelta en un halo de significados morales (Torres Vásquez, 2010: 81).

Lo expuesto no significa que sea imposible aportar un concepto de terrorismo desde una perspectiva jurídica, sino que no es previsible que pueda desarrollarse uno que pueda abarcar íntegramente todo detalle de un fenómeno tan variopinto como éste, ni mucho menos uno que pueda dar soporte a toda la realidad internacional. Pese a ello, los instrumentos internacionales, la jurisprudencia y la doctrina han sumado esfuerzos para construir una definición lo más íntegra posible sobre lo que es el terrorismo. A continuación, se exponen algunos ejemplos propuestos a nivel institucional:

- **RAE**: Desde una arista gramatical, el Diccionario de la Real Academia Española define al terrorismo como una "sucesión de actos de violencia ejecutados para infundir terror" o una "actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos"[2].
- **ONU**: Aunque las Naciones Unidas reconocen la inexistencia de una definición internacionalmente vinculante del término "terrorismo", no se ha desistido en el intento de alcanzar un consenso al respecto. Aunque no prosperó como concepto homogéneamente asumido por la comunidad internacional, en su seno se propuso la siguiente definición de terrorismo: "cualquier acto destinado a causar la muerte o lesiones corporales graves a un civil o a un no combatiente, cuando el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un

[1] BALCUENA, M.C. & MONTES, A. (2018: 7-9) proponen que, si la intención es ser lo más precisos posible en la definición del término "terrorismo", se deben tener en cuenta distintas perspectivas: la gramatical, la académica, la jurídica, la política, la psicológica, la criminológica y la de las Naciones Unidas.
[2] No obstante, el Diccionario Panhispánico del Español Jurídico no incluye ninguna entrada para el término "terrorismo". Sí lo hace para la expresión "delito de terrorismo" que, en esencia, transcribe el delito definido en el art. 1.º de la Decisión Marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (2002/475/JAI).

- gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo"[3].
- **EEUU**: El Código de Regulaciones Federales, inserto en la legislación americana, entiende que el terrorismo abarca todo "uso ilegal de la fuerza y la violencia contra personas o bienes para intimidar o coaccionar a un gobierno, la población civil o cualquier segmento de los mismos, para la promoción de objetivos políticos y sociales"[4].
- **UE**: En sede europea, se ha definido al terrorismo como: "los actos intencionados [...] tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de: intimidad gravemente a una población, obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo, o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional"[5].

En Portugal, el terrorismo integra "conductas de terrorismo que comprenden los delitos de terrorismo, delitos relacionados con grupo terrorista, delitos relacionados con actividades terroristas y financiación del terrorismo", de acuerdo con lo dispuesto en el art. 1. I) del Código de Processo Penal. Más completa y determinada es la definición ofrecida por la Ley núm. 52/2003, de combate del terrorismo. En su art. 2, no solo aporta una conceptualización positiva -señalando lo que es un grupo terrorista o una infracción terrorista-, sino negativa -indicando lo que no lo es-; por ejemplo, al especificar que "no se considera grupo terrorista una asociación creada fortuitamente para la comisión inmediata de un delito". Esta forma permite precisar aún más la figura jurídica en cuestión.

A nivel doctrinal, también hay autores que han intentado formular definiciones para hacer frente a la vaguedad del término "terrorismo", con un compuesto de los elementos que conforman las definiciones institucionales que se han citado previamente[6]. No obstante, no hay una definición enteramente satisfactoria de lo que es el terrorismo ni, posiblemente, la habrá, porque no hay una forma única para manifestarse (Laqueaur, 2023). En palabras de Ronczkowski (2018:15), además, no solo debe definirse lo que es terrorismo sino también actividad terrorista y quién lo es; por lo cual afirma que las agencias en que no deben insistir más en un aspecto conceptual que ha cambiado y seguirá cambiando.

1.2. Características heterogéneas del fenómeno terrorista

El terrorismo es fácil de identificar materialmente, no así conceptualmente. Aunque los efectos que produce pueden llegar a ser bastante similares, las causas pueden ser

[3] Citado en el informe del Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio titulado "Un mundo más seguro: la responsabilidad que compartimos", en la que se recomendó explícitamente la adopción de una definición de terrorismo.
[4] Disponible en el Capítulo I, Parte 0, Subparte P, § 0.85 del Code of Federal Regulations.
[5] Art.1 de la Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo.
[6] Autores como SCHMIDT y JONGMAN (1988) propusieron una investigación en la analizaron más de 100 definiciones distintas y, aún así, no lograron resolver ciertas cuestiones que pueden generar confusión: la diferencia entre terrorismo y otras formas de violencia política, la diferencia entre terrorismo y otros delitos, así como la diferencia entre terrorismo y la guerrilla.

completamente distintas[7]. Por eso es aparatoso pensar que se puede englobar todo lo que implica esta modalidad criminal en unas pocas líneas. No obstante lo expuesto, quizá queriendo o quizá sin querer, la técnica para intentar definir dicho fenómeno ha sido apuntar características del mismo. Se puede ilustrar con las acepciones citadas en el apartado previo:

Tabla 1. Características del terrorismo en intentos de conceptualización. Fuente: Elaboración propia.

AUTOR	CARACTERÍSTICAS
RAE	- Sucesión de actos. – Ejecución con violencia. – Pretende infundir terror y alarma social. – Actuación criminal de bandas organizadas. – Reiteración. – Indiscriminación. – Fines políticos.
High Lever Group (ONU)	- Acto (unidad). – Muerte o lesiones como fin. – Dirigido a civiles o no combatientes. – Intimidación a la población o parte de ella como finalidad. – Promoción de motivos políticos y sociales.
EEUU	- Uso ilegal de la fuerza. - Violencia. – Personas y/o bienes son destinatarios del ataque. – Coacción de Gobiernos los y de la población. - Promoción de motivos políticos y sociales.
UE	- Intencionalidad. – Constituye delitos tipificados. – Remisión a Derechos nacionales. – Lesiones a países u organizaciones internacionales. – Finalidades específicas: * Intimidación a la población. * Obligar a realizar o no realizar actos. * Desestabilizar estructuras fundamentales de los países u organizaciones.

Todas las características destacadas pueden ser constitutivas, en efecto, de una actividad terrorista, pero también pueden no serlo. Por ejemplo, no todo acto terrorista se dirige por una organización o grupo de este tipo, como lo evidencia el caso de los “lobos solitarios”, que si bien actúan motivados por los ideales radicales de las organizaciones o grupos terroristas, lo hacen de manera independiente. Estos individuos -que se autoadoctrinan y se autoactivan en cualquier lugar y momento- son más peligrosos que el terrorismo convencional por su mayor imprevisibilidad y su menor preocupación por el riesgo que pueda ocasionar la realización del atentado (Arias Gil, 2018: 52).

Por otra parte, es peliagudo identificar el terrorismo con violencia sin matizar más al respecto. Ciertamente, hay que contextualizar el momento en que se formularon tales propuestas conceptuales. Pero hoy es – o debería serlo- casi impensable hablar de terrorismo sin considerar los medios tecnológicos que han favorecido su perpetración, en cada una de las fases del *iter criminis*. La concepción tradicional y restringida de la

[7] Así lo considera el Magistrado del Tribunal Supremo español GIMÉNEZ GARCÍA, quien afirma que equiparar las causas y los efectos sería “un grave error de valoración con directa incidencia en el error de diagnóstico y por tanto de remedios para acabar con él” (STS 50/2007, de 19 de enero de 2007; Voto Particular).

violencia, entendida como “uso de la fuerza”, ya no basta para abarcar las modalidades del terrorismo tecnológico, salvo que la irrupción ilegitima y forzosa en redes o plataformas virtuales también se entienda por tal. Actualmente, sería necesario incluir en las descripciones sobre el terrorismo la consideración de una violencia digital que, sin enmarcarse en una relación *face to face*, justifique y resalte que en el universo digital también existen acciones con esa naturaleza.

Ahora bien, la violencia con que se relaciona al terrorismo nunca debería subsumirse meramente en el “terror”. Resulta obvio que un ataque terrorista genera sentimientos de este tipo en la población que lo vive en carne propia o, incluso, en aquella que lo presencia a través de los medios de comunicación, pero puede dar lugar a confusiones. Si se circunscribiese solo a ese aspecto, cualquier delito podría ser terrorismo, porque a nadie le resulta indiferente ser víctima o espectador de un hecho delictivo. Y favorecería aún más lo que Meliá (2006: 10) llama un “uso inflacionario del término”. Debe tratarse de un miedo que no produzca el resto de delitos.

Además, normalmente se relaciona con terror aquello que es capaz de afectar la vida o los bienes propios o del entorno. No pasa así cuando se piensa en el supuesto de que tenga acceso a una red social una publicación que justifique un comportamiento terrorista y que afecte la tranquilidad o el desarrollo de la personalidad de los usuarios que lo visualicen. Al contrario, genera polémica o debates, pero no es usual que sea objeto de terror. De resumir el terrorismo en ese efecto, los actos que persigan su exaltación dejarían de ser parte del fenómeno. Tampoco se debe seguir incurriendo en el error de situar al terrorismo de una forma concatenada con la política. No se trata de un delito de naturaleza política ni obedece siempre a motivos políticos; se trata de un crimen común que puede responder a otro tipo de factores[8].

Pero no todo es cuestionable, al contrario, hay características muy acertadas. Una de ellas es la indiscriminación que destaca la RAE, lo que sirve para evitar que el “terrorismo”, que hace peligrar un bien jurídico de carácter pluriofensivo (Castro; Gómez & Buil-Gil, 2019: 276) y no individual, acabe abarcando otros hechos que realmente no lo son. Ejemplo de ello es el llamado “terrorismo doméstico”. La violencia de género no debería equipararse con el terrorismo ni siquiera a nivel conceptual, primero, porque no esta dirigida a un sector indiscriminado de la población, sino a un sector concreto de ella –las mujeres que han estado unidas con un vínculo sentimental con el autor del hecho-; segundo, porque no necesita ser etiquetado como terrorismo para constituir un ilícito penal y social muy reprochado y; tercero, porque no obedece a las finalidades que definen al terrorismo. De lo contrario, esto conllevaría un ciclo sinfín de figuras delictivas asumidas como actos terroristas.

También es de apreciar positivamente la inclusión de finalidades como elemento a tomar en cuenta a la hora de elaborar una descripción del terrorismo. Aun cuando supongan la dificultad de delimitar aspectos subjetivos, permiten lindar lo que es terrorismo y lo que no. Lo será cuando suponga una de las finalidades establecidas para ello. En este sentido, resulta mucho mas apropiado una enumeración más clara de ellas, como en el caso de la UE, en contraposición con la escueta mención de “motivos políticos y sociales”. Pero esto es trabajo de las legislaciones propias de cada Estado.

[8] El terrorismo ha demostrado ser un fenómeno que va más allá de lo político. En realidad, es producto de un conflicto profundo, por lo que la descripción que se haga de este fenómeno debe asegurarse de no dar la idea de que la dominación política es el único fin.

Por otra parte, la trascendencia de los ataques terroristas no es dañosa solo para las personas, sino también para los bienes, como acertadamente lo destaca el Código de Regulaciones Federales americano. Un atentado dirigido a una estructura simbólica de una Nación, como el Pentágono en EEUU o el Palacio de la Zarzuela, por ejemplo, cuando se promoviese por una de las finalidades que caracterizan al terrorismo, sería constitutivo de tal crimen aunque no provocase ninguna perdida o lesión humana.

Finalmente, es trascendente recordar que los efectos no son siempre equiparables las finalidades perseguidas a nivel individual o grupal de los terroristas. En muchas ocasiones la finalidad último de estos no es matar a determinada cantidad de personas, ni interceptar transmisiones no públicas de ciertos datos informáticos. De hecho, estos sonlos "daños colaterales" de una intención más profunda; menos visible. La finalidad será intimidar a la población para subvertir el orden establecido, desestabilizar las instituciones o alterar de forma grave la paz pública, siendo esos daños el medio coactivo para conseguirlo. En realidad, la actividad terrorista es una forma de propaganda y declaración de intenciones que adopta muchas formas pero, en la mayoría de los casos, promovida por la cobertura de los medios; logrando no solo proyectar los daños materiales realizados sino incrementando los emocionales también para los que visionan tales comportamientos (Ronczkowski, 2018: 15).

2. Condicionantes sociales y tecnológicos

2.1. Terrorismo como fenómeno criminológico

La materialización del terrorismo, en las múltiples figuras delictivas en que se manifiesta, es, en realidad, el resultado de un proceso mucho más insondable e indeterminado. En el terrorismo está presente una dimensión ideológica que actúa como génesis motivacional de dichos actos (Miró Llinares, F. 2005). Lo que lleva a alguien a querer intimidar a la población, o alterar la paz y sosiego público o el buen orden constitucional, responde a modelos emocionales que intervienen en el proceso.

Los terroristas realmente acaban creyendo que deben actuar como lo hacen porque es el medio "correcto" para defender su raza, su independencia o sus valores religiosos[9] (Sordo Estella, 2016: 81). Para la psicología criminal, los actos terroristas nacen de frustraciones en las que, a su vez, subyacen expectativas no cumplidas[10] Aunque hay otros factores -como el educativo- que pueden catalizar o impulsar este proceso. Así, la frustración conduce al odio y al anhelo de cobrar venganza. De forma que, los estados de crisis personal y de pérdida de autonomía e integridad psicológica incrementan las probabilidades de que alguien pueda ceder ante las "ofertas" de una organización extremista (Torres-Marín, Navarro-Carrillo, Dono & Trujillo, 2017: 137) o, al menos, de sus ideales.

En este punto, resulta interesante que la victimización del sujeto, que produce una percepción aversiva de su entorno, es lo que detectan los captadores de las organizaciones criminales terroristas, que manipularán esas sensaciones. Por eso,

[9] Incluso es usual que consideren que se trata de una conducta "socialmente positiva" y no una criminal (Montero Guerra, J.M., 1997).
[10] Lo cual, como aclaran FERNÁNDEZ –MILLÁN, J.M. & SEIJO, M.D., no significa que el terrorismo esté exento de influencias individuales, como su historia personal o su personalidad (2007: 173).

intentar detectar el proceso de pre-radicalización debería ser la clave para intentar paliar los efectos absolutamente negativos que podría tener a posteriori. De hecho, en múltiples Estados, esta fase "previa" constituye un delito autónomo, por el particular peligro que supone. El mundo digital ha favorecido vertiginosamente estos períodos iniciales del terrorismo. Incluso facilita en gran medida el autoadoctrinamiento, lo cual permite el reforzamiento del sujeto como terrorista y el acercamiento a ideales de ese tipo sin siquiera integrarse en un grupo o contactarse con uno de sus miembros. Esta accesibilidad en la red supone, no solo la obtención o reforzamiento de una nueva conciencia acerca de su entorno y la redefinición de su proyecto de vida (Guirao, 2019: 11), sino la metamorfosis individual de esos ideales radicales, lo cual complicará aún más su identificación.

Lo ideal sería, entonces, que se diseñen medios para intervenir en el momento previo al proceso de radicalización violenta. En el Plan de Acción contra el Terrorismo, de 2005, la UE destacaba la importancia de "evitar que individuos se adhieran al terrorismo, abordando los factores y las causas estructurales que puedan conducir a la radicalización y el reclutamiento". La forma más eficaz de hacer esto es garantizando a la sociedad en su conjunto los medios necesarios para su sana educación y su correcta socialización. Y en el ámbito digital, se deben implementar mecanismos para impedir – en la medida en que sea posible- la disponibilidad en línea de ideas conducentes a la comisión de actos terroristas y reforzar la cultura y educación digital de la población.

2.2. Terrorismo como fenómeno adaptable y flexible

Lo estudiado denota claramente la forma en que el fenómeno del terrorismo constituye una amenaza protagónica en las sociedades actuales, no solo por su extremismo y crueldad, sino por la capacidad de adaptación y transformación de sus actores. Así, la relevancia y mutación se convierten en características básicas en la evolución del fenómeno terrorista (Ministerio de la Presidencia de España, Relaciones con las Cortes e Igualdad, 2019: 13 y 14). Los terroristas saben – y si no, aprenden- a valerse de los medios que tienen a su alcance para potenciar y perfeccionar su capacidad operativa. Esto obliga, a su vez, a las instituciones policiales, judiciales y de inteligencia; a investigar y reforzar sus infraestructuras para ir "al paso" de estos nuevos retos. Se volverá un ciclo, porque las amenazas terroristas multidisciplinares y mutables seguirán intentando eludir los diseños defensivos de los Estados. Pero la respuesta debe seguir siendo contundente y, sobre todo, global y coordinada (Feal, 2001: 70). En este sentido, dice Aznar (2018: 139), "el fenómeno terrorista persiste a la vez que cambia; y no deja de sorprender tanto por la continuidad de los procedimientos con los que se manifiesta como por su capacidad para adaptarse a los entornos cambiantes". Y procede a destacar que este es otro factor que impide una definición de terrorismo que exhaustivamente recoja toda la casuística que se ha generado a lo largo de la historia.

2.3. Terrorismo como fenómeno tecnificado

La accesibilidad y difusión que ha brindado la globalización a las ideologías y los elementos culturales para alcanzar nuevos escenarios se ha agudizado irrevocablemente con el advenimiento de los avances tecnológicos. Si ya era cada vez más factible la movilización a otros lugares, los espacios públicos digitales de información han consolidado esto a una escala mucho mayor. Los medios tecnológicos, en particular el

internet se han ido posicionando como la principal vía de difusión de la información; dejando en segundo plano a los "tradicionales". Y esto es algo de lo que el terrorismo se ha valido cada vez más. Los terroristas han demostrado tener muchas habilidades para el marketing online; para recopilar información de las millones de redes en que se organizan; para localizar transportes, objetivos y horarios a través de internet; para recaudar fondos por medios digitales y; en lo relativo al reclutamiento, se valen de tecnologías interactivas, como salas en línea y cibercafés para atraer más adeptos (Weimann, 2004).

De esta manera, las redes terroristas pueden experimentar un crecimiento exponencial al permitir el contacto y la integración de sus miembros; así como dar lugar a nuevas formas de organización, doctrina y estrategia -construidas y retroalimentadas en entornos virtuales-, demostrando una vez más la flexibilidad y adaptabilidad de esta modalidad criminal (Segoviano, 2005: 115 y 116). Pero peor aún, favorece la radicalización a distancia, lo cual dificulta más su identificación, prevención y control[11]. Y es que, 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, 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[12]. 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 de fácil interceptación por los servicios de inteligencia. Ahora bien, operar en células independientes dificultaría la comunicación entre sí para la planificación de atentados masivos 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 tecnologias de la información y la comunicación 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

[11] No obstante, como advierten JORDÁN y TORRES (2007: 124) en su investigación, el reclutamiento directo en la red y la ejecución de ataques cibernéticos a infraestructuras vitales ("sensibles" para la ciencia informática) constituyen un riesgo y una posibilidad, pero aún no se han producido, porque "Internet juega un papel muy relevante pero de refuerzo, unido a otros factores y procedimientos de captación". Además, continúan diciendo que otra de las funciones de la red es transmitir archivos multimedia que refuerzan el adoctrinamiento ideológico, el sentido de pertenencia y la frustración.

[12] La efectividad de las organizaciones terroristas requiere de un equilibrio entre el secretismo y la existencia de canales de comunicación en toda la red, para que la información que necesitan pueda fluir adecuadamente (Ortolá, C., 2020). Conscientes de ello, los terroristas han comprendido que el dominio informático es una pieza fundamental para sus actuaciones y constantemente emplean medios cada vez más complejos. Utilizando el ciberespacio como nuevo campo de acción, las actividades que los terroristas emprenden en internet son muy variadas, pudiendo clasificarse atendiendo a su función, según SÁNCHEZ-GIL (2021: 410), de la siguiente manera: financiación, propaganda, adoctrinamiento, adiestramiento, comunicación interna, planificación y ejecución.

ido volcando hacia él. Sánchez Medero (2010: 204 y ss.) ha desarrollado una tipología de sitios web en los que los terroristas se han ido manifestando:

- 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 Medi*a 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, 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, 2009).

- 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, 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, 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.

- 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.

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 & Pedreira, 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

[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, incluyendo consejos para perpetrar ataques en países occidentales. Para más información, *vid*. INGRAM, H. "Learning from ISIS's virtual propaganda war for Western Muslims: A comparison of Inspire and Dabiq". En NATO Science for Peace and Security Series - E: Human and Societal Dynamics, vol. 136, 2017.

su sencilla accesibilidad son valoradas por los terroristas para el desarrollo de sus actividades.

- 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, 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 español (art. 573), 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.

3. Áreas tecnológicas especialmente problemáticas en el ciberterrorismo

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.

3.1. 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, 2016: 373-375).

Hasta tiempos recientes, *Twitter* (que actualmente se llama “X”) 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 puede notar 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.
- 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:

- 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.
- 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.
- 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.

3.2. 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 recipiente 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[14], con una estructura y jerarquía similar a los foros tradicionales disponibles en la *surface web* (Yuste, 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

[14] 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[14]. 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 encontramos: 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.

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[15].

3.3. Los activos virtuales o criptomonedas

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

[15] En este sentido, Gónzalez Navarro 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 "La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo". En *Revista Española de Derecho Internacional*, vol. 68, núm. 2, 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 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.

virtuales[16]. 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 de policía cibernética.

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[17]. 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. La difícil identificación de las partes y el escaso control que propugnan 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.

Las estadísticas muestran tasas de aumento anuales en la comisión de delitos con criptomonedas, conocidos coloquialmente como “criptodelitos”. Así lo evidencia el Crypto Crime Report de 2023, elaborado por Chainalysis, donde se refiere el volumen de transacciones ilícitas que han tenido lugar en los últimos años. Pese a la crisis que ha tenido el mercado de las criptomonedas en dicho período de tiempo, se muestra una tendencia alcista. Esto es particularmente notorio en lo que respecta al terrorismo, complicándose aún más la situación en tanto su comportamiento en el ámbito financiero “es difícil de distinguir de sus homólogos respetuosos de la Ley” (Ruipérez Canales, J., 2020: 149). 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[18].

[16] 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/

[17] De acuerdo con Rothe y Friedrichs (2015: 3), los crímenes de la globalización - en los que se enmarcan los criptodelitos- y el control de los mismos solo pueden entenderse a partir de una teoría integrada y multidimensional del crimen.

[18] Vid. González Cussac, 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

3.4. El Metaverso

El ecosistema virtual del Metaverso, 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 interactuar con otros, jugar, trabajar, educarse, entre otras[19]. De esta forma, el Metaverso supone un nuevo paradigma de las interrelaciones sociales e interesa atender jurídicamente lo que está ocurriendo allí[20]. Las tecnologías hápticas 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. Ahora bien, 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.

[19] 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.

[20] *Vid.* Serrano Acitores, Metaverso y Derecho. Editorial Tecnos. También, Trallero Masó & Tomas Román,. Metaverso y Derecho Penal. En La Ley Penal, Nº 158, 2022.

4. Conclusiones

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 sistemática. La técnica más empleada en el Código Penal para tipificar los delitos de terrorismo a partir de nuevas tecnologias 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; aunque permite una ubicación sistemática más intuitiva. 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 *Big Data* 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[21].

[21] 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.

Por otra parte, se debe incidir en la pauta fijada por la Estrategia Nacional contra el Terrorismo de 2019 de España. 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*"[22]. 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.

[22] 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.

Referências Bibliográficas

Arias Gil, E. (2018). El futuro del terrorismo nuclear en la táctica de los actores individuales. *Revista del Instituto Español de Estudios Estratégicos*, 12.

Aznar, F. (2018). Repensando el terrorismo. Boletín IEEE, 11. 134–153.

Balbuena, M. C., & Montes, A. (2018). Nuevas tecnologías y traducción de textos sobre terrorismo global: el uso de AntConc para la gestión terminológica (alemán-español). *Futhark. Revista de Investigación Y Cultura*, 13, 3–35. https://doi.org/10.12795/futhark.2018.i13.01

Cancio Meliá, M. (2006). De nuevo: ¿"Derecho penal" del enemigo?. In M.Cancio Meliá & G.Jakobs (Org.), *Derecho penal del enemigo. El discurso penal de la exclusión*. Editorial Edisofer, 341–382.

Cano Paños, M. A. (2019). La violencia terrorista como espectáculo en internet: una aproximación criminológica. *Revista Científica General José María Córdova*, *17*(28).

Castro, F., Gómez, A., & Buil-Gil, D. (2019). La Criminología que viene. *Resultados del I Encuentro de Jóvenes Investigadores en Criminología*. Red Española de Jóvenes Investigadores En Criminología.

Feal, J. (2002). Terrorismo internacional. *Boletín de Información*, 275.

Fernández-Millán, J. M., & Seijo, M. D. (2007). El terrorismo. Una explicación del fenómeno desde la psicología social. *Publicaciones de La Facultad de Educación Y Humanidades Del Campus de Melilla*, 37, 171–189. https://doi.org/10.30827/publicaciones.v37i0.2278

González Cussac, J. L. (2013). Tecnocrimen. In J.L.González Cussac, M.L.Cuerda Arnau (Dir), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Valecia: Tirant Lo Blanch, 205-241.

González Navarro, A. (2018). El uso de nuevas tecnologías en la investigación de delitos de terrorismo. In A.Lima & Cuerda, M.L. (Dir), *Terrorismo, sistema penal y derechos fundamentales,* 543-578). Valencia: Tirant lo Blanch.

Guirao, M. C. (2019). La ciberradicalización: una nueva forma de victimización. *Revista de Internet Derecho Y Política*, 29. https://doi.org/10.7238/idp.v0i29.3171.

Ingram, H. J. (2017). Learning from ISIS's virtual propaganda war for western Muslims: A comparison of inspire and Dabiq, *NATO Science for Peace and Security Series: E:Human and Societal Dynamics,* 136, 170-181, IOS Press.

Jordán, J., & Torres, M. (2007). Internet y actividades terroristas: el caso del 11-M. *El Profesional de La Informacion*, *16*(2), 123–130. https://doi.org/10.3145/epi.2007.mar.04

Laqueur, W. (2003). *Una historia del terrorismo, 4*, Barcelona: Ediciones Paidós.

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

Membiela-Pollán, M. E., **& Fernández, N.** (2019). Herramientas de Marketing digital y competencia: una aproximación al estado de la cuestión. *Atlantic Review of Economics*, *3*(3).

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad de España (2019). *Estrategia Nacional Contra el Terrorismo,* Madrid: Catálogo de Publicaciones de la Administración General del Estado.

Miró Llinares, F. (2005). Democracias en crisis y Derecho penal del enemigo: política criminal frente al terrorismo en los Estados Democraticos antes y después del 11 de septiembre de 2001. *Cuadernos de Política Criminal*, 87, 185–228.

Montero Guerra, J. M. (1997). Análisis psicológico del terrorismo. *Anuario de Psicología Jurídica*, *7*(1), 95–108.

Morán Blanco, S. (2017). La ciberseguridad y el uso de las Tecnologías de la Información y la Comunicación (TIC) por el terrorismo. *Revista Española de Derecho Internacional*, *69*(2), 195–221. https://doi.org/10.17103/redi.69.2.2017.1.08
Ortolà Boscà, C. (2020). Así son las redes terroristas más eficientes según las Matemáticas. *Global Strategy Reports*, *1(*53).
Rodríguez, J. A. (2004). La red terrorista del 11M. *REIS: Revista Española de Investigaciones Sociológicas*, 107.
Rodríguez Morales, T. (2021). El terrorismo y nuevas formas de terrorismo. *Espacios Públicos*, *15*(33).
Ronczkowski, M. R. (2017). Understanding and Defining Terrorism, In M.R.Ronczkowski (Org.), *Terrorism and Organized Hate Crime*, 4, Boca Raton: CRC Press.
Rothe, D., & Friedrichs, D. (2020). Crimes of globalization and the criminological enterprise. In D.Rothe & D.Friedrichs, *Crimes of Globalization*, Chapter 1, New York: Routledge.
Ruipérez Canales, J. (2019). Terrorism financing and the crime-terror relationships as challenges for security in Europe. In Ruggiero, V. (Ed.), *Organized Crime and Terrorist Networks,* 141-155, New York: Routledge.
Sánchez Gil, L. M. (2021). Repensando el concepto de ciberterrorismo. *Boletín Instituto Español de Estudios Estratégicos*, 21.
Sánchez Medero, G. (2010). La nueva estrategia comunicativa de los grupos terroristas. *Revista Enfoques*, *8*(12), 201–215.
Segoviano , S. (2005). Al Qaeda en la red. *Papeles de Cuestiones Internacionales*, 89, 115–122.
Serrano Acitores, A. (2022). *Metaverso y Derecho*. Madrid: Editorial Tecnos.
Somiedo, J. P. (2015). La estructura y organización de los grupos terroristas bajo la óptica del aprendizaje organizacional. *Instituto Español de Estudios Estratégicos*, 24.
Sordo Estella, L. M. (2016). Psicología del terrorismo: breve apunte. *Revista Del Instituto Español de Estudios Estratégicos*, 8, 71–101.
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, 370–384.
Torres-Marín, J., Navarro-Carrillo, G., Dono, M., & Trujillo, H. M. (2017). Radicalización ideológico-política y terrorismo: un enfoque psicosocial. *Escritos de Psicología*, *10*(2), 134–146. https://doi.org/10.24310/espsiescpsi.v10i2.13184
Torres-Soriano, M. R. (2007). La dimensión propagandística del terrorismo yihadista global. Universidad de Granada.
Torres Vásquez, H. (2010). El concepto de terrorismo, su inexistencia o inoperancia: la apertura a la violación de Derechos Humanos. *Diálogos de Saberes: Investigaciones Y Ciencias Sociales*, 32, 77–90.
Trallero Masó, A., & Tomás Román, E. (2022). Metaverso y Derecho Penal. *La Ley Penal,* 158.
Weimann, G. (2004). Terrorismo e internet. *Etic@Net: Revista Científica Electrónica de Educación Y Comunicación en la Sociedad Del Conocimiento*, 3.
Yuste, C. (2015). Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas. Universidad Internacional de La Rioja.

Sobre a Autora

Samar Francisco Agra

Foi agraciada com uma Bolsa de Assistente para exercer funções como Auxiliar de Investigação no Instituto de Ciências Penais e Criminológicas (ICPC) da Universidade Central da Venezuela. Também recebeu uma Bolsa de Iniciação à Investigação na Universidade de Granada, no âmbito da qual realizou um estudo sobre o terrorismo tecnológico. Esta investigação culminou com a realização de uma tese de doutoramento, para a qual lhe foi concedida uma Bolsa de Formação de Professorado Universitário (FPU), que lhe permitiu combinar as suas atividades de investigação no Departamento de Direito Penal da Universidade de Granada com funções docentes nas Licenciatura em Direito e em Criminologia. Participou em diversos projetos de investigação, relacionados com o Direito Penal e novas tecnologias, com especial enfoque na cibercriminalidade. Neste momento, é Investigadora Principal de um projeto de investigação sobre criptomoedas e fluxos migratórios. Tem participado na organização de eventos científicos, colaborado na implementação de novas linhas de investigação no referido Departamento, intervindo em Congressos e Jornadas, e escrito diversas obras científicas.

Sobre os CIJ-RP (CIJ Research Papers / Cadernos de Investigação do CIJ)

Os CIJ-RP são uma série de publicações disponibilizadas em linha que dão a conhecer à comunidade a reflexão desenvolvida no âmbito de projetos de investigação, em comunicações e outras atividades científicas, académicas e de formação, da autoria de investigadores do CIJ, de investigadores visitantes e convidados, bem como estudantes de doutoramento e de mestrado da FDUP. Os CIJ-RP são o testemunho do compromisso com o objetivo da ciência aberta, ao serviço da sociedade. As línguas de publicação são o português e o inglês, podendo excecionalmente a publicação ocorrer em outra língua.

Sobre o CIJ

O Centro de Investigação Interdisciplinar em Justiça (CIJ) é uma Unidade de Investigação e Desenvolvimento integrada na Faculdade de Direito da Universidade do Porto (FDUP). Ramifica a sua investigação em quatro eixos: (1) Direito, Sociedade e Poder, (2) Negócios, Empresas e Mercados (3) Dinâmicas Transnacionais, Transição Verde e Digital e (4) Crime, Segurança e Vitimação.

CIJ CENTRO DE INVESTIGAÇÃO INTERDISCIPLINAR EM JUSTIÇA