

DERECHO PENAL

ANÁLISIS TEÓRICO-PRÁCTICO DE LAS CONDUCTAS TÍPICAS DEL DELITO DE FINANCIACIÓN DEL TERRORISMO CUANDO INTERVIENEN CRIPTOMONEDAS

Samar Francisco Agra

Departamento de Derecho Penal de la Universidad de Granada

Title: *A Theoretical and Practical Analysis of the Constituent Elements of the Crime of Terrorist Financing Involving Cryptocurrencies.*

Resumen: Las criptomonedas constituyen un canal operativo y estratégico para la financiación del terrorismo, por lo que es una cuestión de máximo interés para los reguladores a nivel mundial. La tipificación del delito de financiación del terrorismo —en España, contenida en el art. 576 del Código Penal— incluye una amplia variedad de verbos rectores que abarcan conductas como recabar, adquirir, poseer, utilizar, convertir y transmitir fondos con fines terroristas; todas ellas susceptibles de ser perpetradas mediando criptomonedas. Este trabajo se centra en analizar el potencial de las criptomonedas para facilitar el financiamiento terrorista, en función de cada uno de los comportamientos típicos que integran el tipo penal. La importancia del estudio radica en alcanzar una comprensión jurídica precisa del fenómeno, así como en contribuir a su adecuada delimitación normativa y a la previsión de posibles escenarios delictivos emergentes.

Palabras clave: criptomonedas, criptoactivos, financiación del terrorismo, minería de criptomonedas, crowdfunding, Dark Web, sistema hawala.

Abstract: *Cryptocurrencies constitute an operational and strategic channel for the financing of terrorism, making this a matter of utmost concern for regulators worldwide. The criminal offense of terrorist financing—as defined in Spain under Article 576 of the Criminal Code—includes a wide range of core actions, such as soliciting, acquiring, possessing, using, converting, and transferring funds for terrorist purposes, all of which can be carried out through the use of crypto-assets. This paper focuses on analyzing the potential of cryptocurrencies to facilitate terrorist financing by examining each of the typical behaviors encompassed by the criminal offense. The relevance of this study lies in achieving a precise legal understanding of the phenomenon, contributing to its appropriate regulatory delimitation, and anticipating emerging criminal scenarios.*

Keywords: cryptocurrencies, cryptoassets, terrorism financing, cryptocurrency mining, crowdfunding, Dark Web, Hawala system.

Sumario: 1. Introducción. 2. Aproximación a la tipificación del delito de financiamiento terrorista. 2.1. Exigencias y lineamientos internacionales sobre la tipificación del delito de financiación del terrorismo. 2.2. El delito de financiación del terrorismo en España. 3. Conductas típicas de la financiación del terrorismo con criptomonedas y otros activos virtuales. 3.1. Recabar. 3.1.1. Financiación colectiva o crowdfunding. 3.1.2. Minería de criptomonedas. 3.2. Adquirir. 3.2.1. Venta de productos y servicios en la *Dark Web*. 3.2.2. Diseño y venta de NFTs. 3.2.3. Financiación estatal. 3.3. Poseer. 3.4. Utilizar. 3.5. Convertir. 3.6. Transmitir. 3.6.1. La actualización del sistema “hawala” para transmitir fondos terroristas. 3.6.2. Casos específicos de transmisión de bienes con fines terroristas. 3.7. Otras actividades. 4. Elementos subjetivos del delito de financiación del terrorismo en el contexto cripto. 5. Conclusiones. 6. Referencias consultadas

1. Introducción

Las magnitudes alcanzadas por el terrorismo lo convierten en una de las mayores amenazas para la seguridad internacional, pero también en un fenómeno de difícil abordaje por sus distintas repercusiones. El terrorismo no ha obtenido un concepto unívoco, válido a nivel internacional y que abarque todas las modalidades posibles¹. Por eso, resulta imprescindible atender los diversos componentes que se presentan en cada caso, lo que supone descomponer el “concepto usual de terrorismo”². Algunas notas generales del terrorismo que son apreciadas por LÓPEZ CALERA³ son las siguientes: supone un atentado a los derechos fundamentales de las personas, se integra por acciones humanas que generan terror, se caracteriza por desplegar una violencia indiscriminada y persigue motivos y fines concretos. La inexacta y vaga noción de terrorismo se proyecta sobre su legislación, dando lugar a una “vis expansiva” que aleja este

¹ S. FRANCISCO AGRA. “Una aproximación al (ciber) terrorismo: Modelos previos y actuales”. *Revista DOCRIM*, núm. 8, 2021, pág. 4 y ss. En dicho artículo se considera cómo los intentos por definir el terrorismo son más bien descripciones que apuntan las características del mismo que, como no podría ser de otra manera, se caracterizan por su amplitud y variedad.

² J.M. PAREDES. “El ‘terrorista’ ante el Derecho penal: por una política criminal intercultural”. *Revista Nuevo Foro Penal*, vol. 6, núm. 74, 2010, pág. 122.

³ N. LÓPEZ CALERA. “El concepto de terrorismo. ¿Qué terrorismo? ¿Por qué el terrorismo? ¿Hasta cuándo el terrorismo?”. *Anuario de Filosofía del Derecho*, núm. 19, 2002, págs. 53-55.

fenómeno de la excepcionalidad⁴, pues abarca cada vez más casuística⁵. Por otra parte, también exige la cooperación internacional pues, en reiteradas ocasiones, da lugar a una modalidad criminal que trasciende las fronteras estatales.

El terrorismo supone un serio reto para cualquier Estado de Derecho, porque actúa como su antípoda. El ambiente que genera el terrorismo y la amenaza latente de que este existe atenta contra los derechos y libertades de los ciudadanos y la estructura estatal considerada supone precisamente lo contrario, la vigencia de estos⁶. El Estado ha de suministrar de forma permanente condiciones de seguridad y sana convivencia a sus gobernados, pero los mismos derechos suponen límites a su potestad punitiva, lo que también alcanza al terrorismo. El problema de este tipo de criminalidad es que “trastoca los cálculos acerca de la seguridad con base en los cuales cada ciudadano puede organizar su vida en libertad”⁷. El terrorismo integra esencialmente ciertos elementos que ponen en jaque al entramado institucional de un Estado social y democrático de Derecho: un componente estructural, basado en una organización no siempre de notoria jerarquía, que perfila y comparte los objetivos a cumplir entre sus miembros y; un componente ideológico, que persigue distintos fines —políticos, económicos, reivindicadores, morales, religiosos, etc.— aunque siempre defendibles con la violencia y el amedrentamiento del resto de integrantes de la comunidad⁸.

⁴ C. LAMARCA PÉREZ. “Sobre el concepto de terrorismo (A propósito del caso Amendo)”. *Anuario de Derecho Penal y Ciencias Penales*, tomo 46, fasc. 2, 1993, págs. 535 y 536. La autora señala que la indeterminación de un concepto de terrorismo estrictamente jurídico impide diferenciar esta figura penal de otras, como las organizaciones criminales, en algunos casos. En términos similares, H. TORRES VÁSQUEZ. “El concepto de terrorismo, su inexistencia o inoperancia: La apertura a la violación de derechos humanos”. *Diálogos de Saberes*, núm. 32, 2010, pág. 80; afirma que el terrorismo, el acto terrorista y el terrorista son conceptos confusos que puede atemperar la acción de la justicia

⁵ Es remarcable la postura de A. SCHMID. “Frameworks for conceptualising terrorism”. *Terrorism and Political Violence*, vol. 16, núm. 2, 2004, pág. 204; quien considera que una definición más acotada de terrorismo, que excluya más que incluya, sería más efectiva en la comunidad internacional y tendría menos objeciones materiales.

⁶ J. TERRADILLOS. “El Estado de Derecho y el fenómeno del terrorismo”. *Terrorismo y Estado de Derecho*. Editorial Iustel, José Ramón Serrano y Eduardo Demetrio (dirs.), 2010, pág. 272. La Estrategia Nacional contra el Terrorismo española del año 2019 transmite claramente la pugna entre el terrorismo y el Estado de Derecho. Por una parte, sugiere la actuación conjunta de todas las instituciones públicas para luchar contra el terrorismo, como consecuencia de tratarse de un Estado así categorizado. Por otra, reconoce la desaparición de ETA “como muestra de la victoria del Estado de Derecho contra la barbarie terrorista”. GOBIERNO DE ESPAÑA. Estrategia Nacional contra el Terrorismo, 2019, págs. 22 y 75.

⁷ J. PÉREZ ROYO. “La democracia frente al terrorismo global”. *Terrorismo, democracia y seguridad, en perspectiva constitucional*. Editorial Marcial Pons, Javier Pérez Royo (dir.) y Manuel Carrasco Durán (coord.), 2010, pág. 9.

⁸ E. BORJA. “Justicia penal preventiva y Derecho penal de la globalización: proyecciones en el ámbito del terrorismo”. En *Anuario de Derecho Penal y Ciencias Penales*, núm. 70, 2017, pág. 54. No tiene dudas el autor cuando señala que por más inmoral que resulte una organización, no podrá definirse como terrorista si sus mecanismos de actuación son pacíficos. En todo caso, los terroristas instrumentalizan la violencia.

Considera ACALE SÁNCHEZ⁹ que el terrorismo ha seguido siendo considerado como una manifestación criminal peligrosa y temida, no solo por su aumento y reiteración, sino por el rechazo social que supone el autor individual o grupal y su comportamiento¹⁰. Esto se ha extendido al legislador, quien ha establecido una respuesta penal y penitenciaria rígida y no necesariamente muy efectiva. Si bien no siempre ha sido posible, la vocación internacional que suele tener el terrorismo ha suscitado el interés por una política criminal común y cohesionada. Como resultado, las normativas antiterroristas del mundo comparten ciertos aspectos: un adelantamiento de la punibilidad, con la sanción de actos preparatorios; la utilización de términos vagos y excesivamente inclusivos que, en muchos casos, puede colisionar con los principios de legalidad y seguridad jurídica; la imposición de penas desproporcionadas y; la tipificación de delitos de pertenencia o colaboración con una organización o grupo terrorista¹¹. De esta forma, el análisis y tratamiento político-criminal del terrorismo genera polarizaciones de opinión¹² que son difíciles de saldar y mantienen abierto el debate.

Lo dicho hasta ahora es particularmente cierto con la aparición de las nuevas tecnologías, pues el Internet dio lugar a un espacio idóneo para el desarrollo y transformación del fenómeno en cuestión¹³. Los avances tecnológicos han cambiado radicalmente la forma de entender el terrorismo¹⁴, permitiendo su expansión mundial y facilitando —y hasta econo-

⁹ M. ACALE SÁNCHEZ. “Terrorismo y tratamiento punitivista: más allá de la prisión”. *El terrorismo en la actualidad: un nuevo enfoque político criminal*, Ana Pérez Cepeda (dir.). Editorial Tirant Lo Blanch, 2018, pág. 435.

¹⁰ Múltiples estudios sobre el terrorismo se centran precisamente en el rechazo social que suscita. Un ejemplo de ello es el de E. OREHEK; S. et.al. “Need for Closure and the Social Response to Terrorism”. *Basic and applied social psychology*, núm. 32, 2010, pág. 289; el cual concluyó, basándose en los resultados de cinco experimentos, que el terrorismo genera una reacción psicológica aversiva en la sociedad que impulsa a los individuos a formar sistemas de creencias protectoras de cierre. Más explícito aun es el trabajo de R. ROSENFELD. “Terrorism and Counter-Terrorism: Criminological perspectives”. *Sociology of Crime, Law and Deviance*, El Sevier, vol. 5, 2004, pág. 30; donde se expone que el terrorismo concierne una “cruzada moral” que persigue el cambio de estatus social para los actores que lo llevan a cabo. Lo anterior se acrecienta con la aparición de las nuevas tecnológicas, en concreto las redes sociales que conforman un espacio crítico donde las personas drenan y procesan en conjunto los incidentes terroristas. *Vid.* V. BOVE; et.al. “The emotional effect of terrorism”. *Scientific Reports*, núm. 14, 2024. Recuperado de la versión electrónica disponible en el siguiente enlace: <https://www.nature.com/articles/s41598-024-77350-5>.

¹¹ A. PÉREZ CEPEDA. “Política criminal contra el terrorismo en la actualidad”. *Perspectiva multidimensional del conflicto penal: de la política criminal a la concreción normativa “la línea invisible”*, Arnel Medina Cuenca (dir.). Unión Nacional de Juristas de Cuba, 2019, pág. 446.

¹² J. BECERRA-MUÑOZ & D. GARCÍA AGUILAR. “La política criminal antiterrorista en los tribunales”. *Boletín Criminológico*, núm. 5, 2018, pág. 2.

¹³ G. GADEA. “El terrorismo, las nuevas tecnologías y la libertad de expresión en España”. *Revista Pensamiento Penal*, núm. 12, 2015, pág. 85.

¹⁴ T. RODRÍGUEZ MORALES. “El terrorismo y nuevas formas de terrorismo”. *Espacios Pùblicos*, vol. 15, núm. 33, 2012, pág. 84. La autora aplica esta teoría al caso específico

mizando— todas sus actuaciones, desde las más iniciales. La innovación tecnológica no solo permite la compra de artefactos y su envío a distancia, especialmente a través de la Internet oscura, sino que “abre un vasto depósito de información técnica potencialmente relevante a cualquier individuo en cualquier lugar de la Tierra”, impulsando la comunicación entre células terroristas, ofreciendo cursos de capacitación y reclutamiento¹⁵ y enalteciendo los actos ejecutados. También permite a los terroristas manejar su propio contenido y dar publicidad a sus planes e ideales¹⁶. La preocupación por la utilización terrorista de estos medios es la posibilidad de que también resulten en ataques más graves que los conocidos¹⁷. La capacidad tecnológica de los terroristas abre la puerta a ataques más sofisticados, como el uso de drones, ciberataques contra infraestructuras críticas o incluso bioterrorismo. Esto genera preocupaciones significativas sobre el impacto devastador que estas herramientas podrían tener si se usan con fines maliciosos. Todas estas manifestaciones integran el concepto de terrorismo cibernético o ciberterrorismo, que combina técnicas del pasado con el avance técnico moderno de forma sistematizada¹⁸.

En suma, el ciberterrorismo es una forma muy destructiva de delincuencia por su amplia utilidad práctica pues, en la actualidad, casi todas las acciones terroristas pueden dirigirse, depender o apoyarse de medios cibernéticos. Sin exhaustividad, las herramientas informáticas pueden servir para ocasionar daños materiales y físicos, lanzar ataques contra equipos y/o infraestructuras técnicas, hacer propaganda, incitar, amenazar, hacer proselitismo, financiar los ataques y reclutar nuevos

de Al Qaeda. Por su parte, R. LODEIRO. “El uso de las nuevas tecnologías por el terrorismo yihadista”. *Cuadernos de la Guardia Civil: Revista de Seguridad Pública*, núm. 54, 2017, pág. 52, relata el aprovechamiento que de las nuevas tecnologías y el Internet han emprendido ISIS y DAESH. Fruto de las labores antiterroristas, no obstante, muchas de sus cuentas han sido clausuradas, tras concienciar a los rastreos por parte de las autoridades.

¹⁵ L. CHIN-HUANG; D. LIOU & K. WEI WU. “Opportunities and challenges created by terrorism”. *Technological Forecasting and Social Change*, vol. 74, núm. 2, 2007, s/p. Recuperado de la versión electrónica disponible en el siguiente enlace: https://www.sciencedirect.com/science/article/abs/pii/S0040162506000527?casa_token=-9DG40BVvC8AAAAA:GDrOnTY8tCJOia8_nyDQ0WmCmLxCd2SmZ6RmCY8uNW20S-my1dfsel30v6Qpy3ntCyn_B5TUm2gXI. Como advierten M. POVEDA & B. TORRENTE. “Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista”. *Opción*, año 32, núm. esp. 8, 2016, págs. 515 y 516; hay múltiples páginas webs donde se ofrece reclutamiento clandestino e instrucciones para llevar a cabo actos terroristas, por ejemplo para establecer una organización clandestina o ejecutar una toma de rehenes.

¹⁶ G. WEIMANN. “Terrorismo e Internet”. *Etic@ net*, núm. 3, 2010, pág. 2.

¹⁷ W. KOH. “Terrorism and its impact on economic growth and technological innovation”. *Technological Forecasting and Social Change*, vol. 74, núm. 2, 2007. Versión electrónica recuperada del siguiente enlace: https://www.sciencedirect.com/science/article/abs/pii/S0040162506000072?casa_token=yzLJzHMCad4AAAAA:n7Ai7vLYx1r7vtxoQSW7jkwO0E Dy4b0i2DEGWx0XkNkGJW-QBBs4IDKSMqkv2NBLmtnFonQ4dh9w.

¹⁸ R. ARIAS & L. MANZANO. “El terrorismo y su transformación”. *Revista Academia de Guerra del Ejército Ecuatoriano*, vol. 16, núm. 1, 2023, pág. 138.

colaboradores¹⁹. En este contexto, uno de los aspectos más preocupantes y de creciente relevancia es el del financiamiento terrorista mediante criptomonedas. Las criptomonedas son un tipo de activos virtuales —en tanto son medios digitales de intercambio y de pago— sin soporte físico, pues existen y funcionan únicamente en Internet²⁰. No tienen una existencia física ni un respaldo material, por lo que su funcionamiento depende estrictamente de sus atributos y basamentos computacionales. Se fundamentan en algoritmos matemáticos y técnicas de encriptación que permiten salvaguardar registros y transmitir datos de forma privada, es decir, sin intervención de las autoridades u otros intermediarios. Dichos registros se plasman y difunden a través de tecnologías de registro distribuido, como *blockchain*. Cada criptomoneda tiene su propia cadena de bloques, donde cada bloque contiene un conjunto de transacciones confirmadas. Así, el funcionamiento de las criptomonedas involucra la participación de distintos usuarios y agentes que participan en la red, que se define como un conjunto de ordenadores que están interconectados, pudiendo establecer comunicaciones entre ellos y compartir datos y recursos, independientemente de la localización física de los dispositivos conectados; cada uno de los cuales se denominan nodos. Cuando un nodo (uno de esos ordenadores) realiza una transacción con criptomonedas, dicha información se transmite a través de la red. En ese momento, un grupo de otros nodos, que son los llamados mineros, deben proceder a validar las transacciones en una especie de gran libro de registro —conocido como *blockchain*—, a cambio de lo cual reciben incentivos.

Este trabajo centra su atención en dicho fenómeno, analizando cómo los activos digitales pueden ser utilizados por organizaciones terroristas para transferir fondos, eludir controles financieros tradicionales y dificultar el rastreo por parte de las autoridades.

2. Aproximación a la tipificación del delito de financiamiento terrorista

2.1. Exigencias y lineamientos internacionales sobre la tipificación del delito de financiación del terrorismo

Dentro de todas las manifestaciones del terrorismo basado en herramientas tecnológicas, es especialmente crucial hacer referencia a la

¹⁹ V. PONS GAMÓN. “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”. *URVIO: Revista Latinoamericana de Estudios de Seguridad*, núm. 20, 2017, pág. 85.

²⁰ U. CHOCHAN. “A history of Bitcoin”. En *Critical Blockchain Research Initiative, Discussion Paper Series: Notes on the 21st Century*, 2022, pág. 9.

financiación de tales actividades. Esta dotación de recursos se ha identificado como el alma del terrorismo y/o de su propagación²¹, por ser el punto de partida que permite la estructuración y operatividad de estos delincuentes. Sin recursos económicos, no podrían sustanciar todas sus actividades; al menos no con la misma eficiencia. El terrorismo es, mayoritariamente, un proceso prudente y planificado con recursos limitados²². Por esa razón, es lógico que las instituciones y herramientas diseñadas para la lucha antiterroristas tengan la financiación como una prioridad. Como mencionan JOHNSON y JENSEN²³, se trata de un problema delictivo tan complejo que tiene pocas buenas soluciones. Pero no por eso se debe menguar la intensidad en la búsqueda de soluciones para esta severa problemática jurídica, pues la cada vez más profesional forma de actuar de los terroristas no puede responderse con dejadez. Especialmente, es útil prestar atención a los individuos y plataformas que usan para ejecutar estos movimientos, ya que normalmente no tienen control absoluto sobre estos y es donde se vuelven más vulnerables a su detección²⁴. Como menciona la Oficina de Lucha contra el Terrorismo de las Naciones Unidas²⁵, la amenaza terrorista se ha recrudecido a nivel mundial en los últimos años, lo que ha supuesto nuevos nexos entre terroristas y nuevas formas de financiación²⁶. El terrorismo es, entonces, un fenómeno dinámico que ha exigido la atención internacional para buscar respuestas.

El Grupo de Acción Financiera Internacional (GAFI) ha dedicado grandes esfuerzos a comprender y prevenir la financiación del terrorismo. Sus Recomendaciones son muy valiosas en este sentido. Pero además, la Unión Europa actúa como filtro entre aquellos y la normativa

²¹ Por ejemplo, M. BUESA. "Financiación del terrorismo". *Economía del Terrorismo*, núm. 893, noviembre-diciembre, 2016, pág. 27; y P. ROMANIUK. "The State of the Art on the Financing of Terrorism". *he RUSI Journal*, vol. 159, núm. 2, 2015, pág. 9. También *vid.* S. CHIBUEZE. "Overview of Terrorist Financing in Nigeria: Legal and Institutional Framework for Combating Terrorism Financing". *SSRN Papers*, 2024, pág. 2.

²² P. TOMPKINS. & N. BOS. *Human factors considerations of undergrounds in insurgencies*. Fort Bragg, North Carolina, United States Army Special Operations Command. 2da Edición, 2013, pág. 317.

²³ J. JOHNSON. & C. JENSEN. "The financing of terrorism". *The Journal of the Institute of Justice & International Studies*, núm. 1, 2010, 108.

²⁴ R. BARRETT. "Preventing the financing of terrorism". *Journal of International Law*, vol. 44, núm. 3, 2012, pág. 724.

²⁵ OFICINA DE LUCHA CONTRA EL TERRORISMO. "Lucha contra la financiación del terrorismo". Naciones Unidas, s/f. Recurso electrónico recuperado del siguiente enlace: <https://www.un.org/counterterrorism/es/cct/countering-the-financing-of-terrorism>. Consultado por última vez el día 10 de julio de 2025.

²⁶ En este sentido, la misma organización internacional ha reconocido en la Resolución 2462 (2019) del Consejo de Seguridad que estos actores criminales aprovechan métodos de pago emergentes, como los activos virtuales. Dicho Consejo ha sido el protagonista absoluto de las Naciones Unidas en materia antiterrorista. *Vid.* J. RUPÉREZ. "Las Naciones Unidas en la Lucha contra el Terrorismo. Primer Balance". *Cuadernos de Pensamiento Político*, núm. 5, 2005, pág. 2.

interna de sus Estados Miembros, por lo que estos se hallan en una situación privilegiada²⁷. Y esto se agradece porque la regulación de delitos de esta magnitud, tan complejos y abarcadores, es una tarea difícil. La mayoría de los textos de ambos organismos muestran una predilección por el enfoque basado en riesgo, es decir, una línea sustancialmente profiláctica. Esto tiene la ventaja de no actuar solo cuando ya se ha producido el daño, que puede ser irreversible, y de ser un modelo regulatorio más dinámico y flexible frente a los constantes cambios del fenómeno. No obstante, la respuesta no siempre puede ser de este tipo, de ahí que la Recomendación 5 del GAFI sea la que sigue: “Los países deben tipificar el financiamiento del terrorismo en base al Convenio Internacional para la Represión de la Financiación del Terrorismo, y deben tipificar no sólo el financiamiento de actos terroristas, sino también el financiamiento de organizaciones terroristas y terroristas individuales, aún en ausencia de un vínculo con un acto o actos terroristas específicos”²⁸. Esto incluye otros niveles de tratamiento: la tipificación y persecución penal.

Así, el GAFI, como creador de estándares globales, propicia una cultura compartida a nivel jurídico-penal a la hora de estructurar el delito de financiación del terrorismo, al igual que el de blanqueo de capitales; así como una sinergia entre el Derecho nacional, el internacional y, en Europa, el supranacional. Tal integración debería ser capaz de promover una cooperación coordinada y basada en un soporte jurídico formado y operativo. Esto no solo fortalece las capacidades individuales de cada Estado, sino que estimula una respuesta lo más unificada posible a una amenaza transnacional. Armonizar las legislaciones y procedimientos es uno de los objetivos de las entidades supranacionales e internacionales para lograr una acción conjunta, no solo para evitar que los terroristas sostengan sus actividades, sino porque el rastro del dinero o los fondos resulta muy útil para identificar a sus autores y apoyos. La cooperación no solo se expresa, no obstante, en la forma en que se tipifican los delitos, sino en las previsiones legislativas y operativas para investigarlos y perseguirlos.

Situando la mirada sobre la UE, ésta ha intentado unificar la preventión y respuesta administrativa y penal de la financiación del terrorismo

²⁷ J. CLAVIJO. *La prevención de blanqueo de capitales. Un análisis teórico-práctico*. J.M. Bosch Editor, 2022, pág. 20.

²⁸ La Resolución 1373 del Consejo de Seguridad de las Naciones Unidas de 2001 ya había decidido, en virtud del Capítulo VII de la Carta de las Naciones Unidas, que todos los Estados “tipifiquen como delito la provisión o recaudación intencionales, por cualesquier medios, directa o indirectamente, de fondos por sus nacionales o en sus territorios con intención de que dichos fondos se utilicen, o con conocimiento de que dichos fondos se utilizarán, para perpetrar actos de terrorismo”. Términos similares utiliza el Convenio Internacional para la Represión de la Financiación del Terrorismo para instar a lo mismo.

en los Estados miembros²⁹. Progresivamente se ha fortalecido el papel de la Unión en la gobernanza antiterrorista, entre otras razones porque no ha habido otra opción: Europa ha sido un espacio muy afectado por el terrorismo y sufrir este tipo de ataques, inevitablemente, da lugar a un aumento en el número de iniciativas para enfrentar este crimen atroz³⁰. Los objetivos de la Unión en este y otros campos se cumplen con distintos tipos de actos legislativos. En lo que respecta al terrorismo, son muchos los que se pueden destacar, pero especialmente la Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo. Este documento reconoció al terrorismo como un delito que debería tipificarse en todos los Estados miembros, en un momento en que solo unos pocos de ellos poseían legislación antiterrorista. Por otra parte, con tal Decisión, la UE se convirtió en el primer actor internacional que acordó una definición común de terrorismo³¹, sobre el que construir la estructura jurídico-punitiva que resulte.

Asimismo, en sede europea se han dictado diversas Directivas relacionadas con el terrorismo, conocidas comúnmente por una denominación secuencial: la 91/308 CEE o Primera Directiva, la 2001/97/CEE o Segunda Directiva, la 2005/60/CE o Tercera Directiva, la Directiva (UE) 2015/849 o Cuarta Directiva y la Directiva (UE) 2018/843 o Quinta Directiva. A estas hay que sumar la Directiva (UE) 2024/1640 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Todas ellas, contextualizándose en la realidad del momento en que fueron dictadas, asientan la lucha antiterrorista en el aspecto económico y el control sobre las diversas fuentes de financiación de los terroristas³².

2.2. *El delito de financiación del terrorismo en España*

La financiación del terrorismo, acordando la actuación punitiva española con los lineamientos internacionales, constituye un delito autó-

²⁹ J. FERRÉ OLIVÉ. "Aspectos conflictivos del delito de lavado de dinero". *Silver Anniversary Book Commemorating the 25th Anniversary of the Faculty of Law and Administration*. Uczelnia Łazarskiego, Stefański (ed.), 2022, pág. 298.

³⁰ C. KAUNERT & S. LEONARD. "The collective securitisation of terrorism in the European Union". *West European Politics*, vol. 42, núm. 2, 2020, pág. 22.

³¹ J. ARGOMANIZ. "Post-9/11 institutionalisation of European Union counter-terrorism: emergence, acceleration and inertia". *European Security*, vol. 18, núm. 2, 2009, pág. 6.

³² Y. ALONSO. "La posición de la Unión Europea tras el 11-S. Revisión 'normativa' sobre prevención y cooperación frente al terrorismo". *Comillas Journal of International Relations*, núm. 26, 2023, pág. 70.

nomo según el Código Penal del país, tipificado en España en el artículo 576. Tal precepto indica que será castigado con pena de prisión de cinco a diez años y multa del triple al quíntuplo de su valor “el que, por cualquier medio, directa o indirectamente, recabe, adquiera, posea, utilice, convierta, transmita o realice cualquier otra actividad con bienes o valores de cualquier clase con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte, para cometer cualquiera de los delitos comprendidos en este Capítulo”; es decir, algún delito terrorista. Este delito, como no podría ser de otra manera, abarca diversas conductas delictivas que a grandes rasgos abarcan la obtención, posesión o disposición de fondos. Pueden ser cometidas por sujetos individuales y/o por personas jurídicas³³, de forma dolosa o imprudente³⁴. Además, al hacer referencia a cualquiera de los delitos terroristas, el tipo penal básico da un tratamiento unitario tanto a la financiación de organizaciones terroristas como de actos terroristas³⁵. Al ser un delito de mera actividad, la consumación del delito se produce con el manejo de los fondos a través de cualquiera de los verbos rectores del precepto y su agotamiento cuando son efectivamente empleados para los fines terroristas previstos³⁶. Por tanto, tampoco es necesaria la pertenencia ni relación con una organización terrorista, sino que basta con tener el propósito de favorecer finalidades terroristas y movilizar fondos hacia esa causa³⁷.

Sin entrar a valorar con profundidad cada conducta típica, sobre lo cual se hará referencia en el apartado que sigue, sí se incidirá ahora en el objeto material del delito. El legislador habla de “bienes o valores de cualquier clase”. En la historia legislativa del delito se llegó a hablar de

³³ 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; extendió la responsabilidad penal de las personas jurídicas por cualquier delito terrorista, ya no solo por la financiación de actividades de este tipo.v

³⁴ M.A. CANO PAÑOS. “La reforma de los delitos de terrorismo”. *Estudios sobre el Código Penal Reformado (Leyes Orgánicas 1/2015 y 2/2015)*. Lorenzo Morillas (dir.). Editorial Dykinson, 2015, págs. 931 y 932.

³⁵ J. GONZÁLEZ CUSSAC & C. VIDALES RODRÍGUEZ. “El nuevo delito de financiación del terrorismo: consideraciones acerca de su necesidad y conveniencia”. *Financiación del terrorismo, blanqueo de capitales y secreto bancario: un análisis crítico*. José Luis González Cussac (dir.). Editorial Tirant Lo Blanch, 2009, págs. 187 y 188.

³⁶ I. BLANCO CORDERO. “¿Es necesario tipificar el delito de financiación del terrorismo en el Código Penal español?”. *Athena Intelligence Journal*, vol. 4, núm. 1, 2009, pág. 52. El agotamiento del delito da lugar al subtipo agravado del delito, contenido en el art. 576.2 CP: “Si los bienes o valores se pusieran efectivamente a disposición del responsable del delito de terrorismo, se podrá imponer la pena superior en grado. Si llegaran a ser empleados para la ejecución de actos terroristas concretos, el hecho se castigará como coautoría o complicidad, según los casos”.

³⁷ M. CANCIO MELIÁ. *Los delitos de terrorismo: Estructura típica e injusto*. Editorial Reus, 2010, pág. 256.

“fondos”³⁸. No obstante, con el avance de la tecnología, la globalización, y el uso de nuevas herramientas financieras, los terroristas tienen acceso a una gama más amplia de recursos para financiar sus actividades. Por eso, la actual configuración típica utiliza una denominación genérica que refiere tanto a cosas, como a derechos crediticios o patrimoniales que suministran beneficios a su poseedor. Con esto se pretende mantener la efectividad del tipo penal frente a las nuevas tendencias internacionales, como el surgimiento y utilización de los criptoactivos³⁹. De forma que es irrelevante la forma en que se presente el objeto, pudiendo ser tangible o intangible; material, electrónico o digital⁴⁰. Después de todo, el art. 576.3 CP agrava el injusto y el tratamiento penológico del delito de financiación del terrorismo cuando en su ejecución media extorsión, falsedad documental o cualquier otro delito. Cuando se produce una duplicidad típica con el apartado 1, MUÑOZ CONDE⁴¹ considera que la solución es aplicar el principio de alternatividad y se castigaría por el delito más gravemente penado.

Las criptomonedas, por su naturaleza descentralizada y potencial global, pueden desempeñar un papel crucial en la perpetración del delito de financiamiento terrorista⁴². En la mayoría de los casos, su fácil conversión a dinero fiduciario y viceversa puede facilitar la ocultación del origen de los fondos y propiciar movimientos discretos y rápidos, con difícil rastreo por parte de las autoridades. Esto permite a las organizaciones terroristas operar de manera mucho más discreta y eficaz a nivel financiero, lo que representa un desafío significativo para las autoridades que buscan prevenir el financiamiento del terrorismo. Además, se reproducen en este ámbito las problemáticas observadas por PÉREZ MEDI-

³⁸ El Fondo Monetario Internacional en las “Notas de redacción sobre cuestiones específicas: Tipificación del financiamiento del terrorismo como delito” establecía con claridad que el término “fondos” debía entenderse tan genéricamente como el término “bienes”, incluyendo servicios y recursos financieros o económicos de toda índole.

³⁹ F. NAVARRO CARDOSO. “Los tipos dolosos del delito de financiación del terrorismo”. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 20, 2018, págs. 14 y 15.

⁴⁰ J. DEL CARPIO. “El objeto material del blanqueo de capitales en la Directiva 2018/1673: a la vez, sobre la necesidad o no de modificar el Código penal para dar cabida a las nuevas formas en las que puede representarse”. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 25, 2023, págs. 7 y 8.

⁴¹ F. MUÑOZ CONDE. *Derecho Penal, Parte Especial*. Editorial Tirant Lo Blanch, 23^a ed., 2021.

⁴² En el trabajo de R. ANGGRIAWAN & M. ENDRIYO. “Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations”. *Novum Jus*, vol. 18, núm. 2, 2024; se expone que los atributos inherentes a las criptomonedas facilitan y agilizan la ejecución de operaciones intrincadas de financiación del terrorismo. Es decir, esta tecnología es aprovechable por los terroristas porque hace que sea relativamente sencillo llevar a cabo tareas que antes eran mucho más exigentes a nivel logístico-operativo. Además, explican E. FLETCHER; C. LARKIN & S. CORBET. “Countering money laundering and terrorist financing: A case for bitcoin regulation”. *Research in International Business and Finance*, vol. 56, 2021, s/p. Recurso electrónico recuperado el siguiente enlace: <https://www.sciencedirect.com/science/article/abs/pii/S0275531921000088>.

NA⁴³ sobre la delincuencia con criptomonedas: no en todos los países se cometen los mismos delitos con criptomonedas, hay escasa jurisprudencia en la materia y limitado conocimiento sobre las cuestiones técnicas de aquellas por parte de los operadores jurídicos y los sistemas de seguridad que sostienen las criptomonedas dificultan la potencial reacción de las autoridades policiales y judiciales.

Finalmente, sobre la imprudencia se pronuncia el art. 576.4 CP únicamente para los que estando sujetos por la Ley para colaborar con las autoridades para prevenir actividades de financiación del terrorismo no cumplan con tales obligaciones; en este caso, es particularmente relevante los prestadores de servicios con criptoactivos. Es evidente que hay un límite subjetivo concreto para la modalidad imprudente; no así con la modalidad dolosa⁴⁴. Especial atención merece también la apreciación de ABEL SOUTO⁴⁵, al afirmar que el tratamiento penológico de la modalidad imprudente de la financiación del terrorismo es un “exceso” que solo puede justificarse por estar dirigido a quienes se encuentran en posición de garante. En este sentido, confiere especial importancia el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos. Modifica la Directiva (UE) 2015/849, por lo que da especificidad a la gestión de riesgos de tales delitos cuando son perpetrados con activos virtuales. La nueva normativa amplía los sujetos obligados por la normativa de blanqueo de capitales, a todos los proveedores de servicios de criptoactivos incluidos en el llamado Reglamento MiCA⁴⁶ —no solo a los de custodia de monederos electrónicos y los de intercambio de criptomonedas por monedas fiduciarias— y establece obligaciones específicas para cada uno.

El último Reglamento mencionado requiere a tales proveedores autorización por la autoridad competente, para lo cual deberán cumplir determinados requisitos; los cuales se endurecen en los casos de prestación de servicios de custodia⁴⁷. Por ejemplo, junto a la solicitud tendrán que definir

⁴³ D. PÉREZ MEDINA. “Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo”. *Boletín Criminológico*. Edición especial, núm. 206, 2020, págs. 20 y 21.

⁴⁴ I. BLANCO CORDERO. “La modalidad imprudente del delito de blanqueo de capitales”. *VI Jornadas sobre prevención y represión del blanqueo de capitales*. Abogacía Española, 2018, pág. 16. Recurso electrónico recuperado del siguiente enlace: <https://www.abogacia.es/wp-content/uploads/2018/12/3delitoblanqueo.pdf>. Consultado por última vez el día 10 de julio de 2025.

⁴⁵ M. ABEL SOUTO. “Las reformas penales de 2015 sobre el blanqueo de dinero”. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 19-31, 2017, pág. 34

⁴⁶ Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos.

⁴⁷ J. MARTÍ. “La propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos: La propuesta MiCA”. *Revista de Derecho del Sistema Financiero*, núm. 1, 2021, pág. 478.

procedimientos de control interno. SUÁREZ DE LEZO⁴⁸ entiende por tal un manual relativo al lavado de dinero y el financiamiento terrorista, a la protección de datos personales o a las brechas de seguridad. De esta forma, proporciona una base sólida de regulación sobre la emisión, funcionamiento, organización y gobernanza de los proveedores de servicios con criptoactivos⁴⁹. Para proteger la seguridad del mercado criptográfico y sus usuarios, el art. 59.5 Reglamento MiCA establece que “ninguna persona que no sea un proveedor de servicios de criptoactivos podrá utilizar un nombre o una razón social, emitir comunicaciones publicitarias o valerse de cualquier otro procedimiento que sugiera que es un proveedor de servicios de criptoactivos o que pueda crear confusión al respecto”. Es trascendente, atendiendo a lo expuesto, la relevancia de los programas de cumplimiento normativo —o *compliance*— para evitar la comisión de la financiación del terrorismo en su modalidad imprudente. Además, es crucial aplicar medidas de diligencia debida, como el *Know Your Customer* y la regla de viaje⁵⁰. De hecho, esto sigue la línea de la tercera estrategia propuesta por BEDECARRATZ⁵¹ para hacer frente al potencial delictivo de las criptomonedas. Algunas jurisdicciones como Abu Dabi y EEUU establecen la obligatoriedad de establecer este sistema preventivo, con un enfoque basado en riesgos y monitorización de movimientos.

3. Conductas típicas de la financiación del terrorismo con criptomonedas y otros activos virtuales

Tras la reforma del Código Penal del año 2015, las formas de comisión del delito de financiación del terrorismo se ampliaron, abarcando conductas similares a las previstas en la configuración del blanqueo de capitales pero mercedoras de una mayor pena por la gravedad que supone el terrorismo⁵². No obstante, son independientes a los verbos rectores de aquel delito, aunque puede ser posible que ambos se perpetren de forma paralela dando lugar a un concurso ideal, ya que protegen bienes jurídicos diferen-

⁴⁸ SUÁREZ DE LEZO. “Principales implicaciones del Reglamento MiCA para las entidades del mercado de criptoactivos”. *CMS Albiñana*, 2023, pág. 2.

⁴⁹ F. SANTANDREU. “Criptomonedas: ¿regular o no regular en el nivel español y europeo? He ahí la cuestión”. *Revista Universitaria Europea*, núm. 39, 2023, pág. 173

⁵⁰ Se refiere a la obligación de los proveedores de servicios de criptoactivos de compartir información de quien envía y quien recibe una transacción para que, si es necesario investigarlo, se facilite el rastreo y bloqueo de movimientos sospechosos.

⁵¹ F. BEDECARRATZ. “Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal”. *Revista Chilena de Derecho y Tecnología*, vol. 7, núm. 1, 2018.

⁵² J. MORCILLO JIMÉNEZ. “Delitos contra el orden público”. *Lecciones de Derecho Penal, Parte Especial*. Elena Marín de Espinosa (dir.). Editorial Tirant Lo Blanch, 4^a ed., 2023, pág. 787.

tes⁵³. A continuación se hará un breve desglose de cómo las numerosas conductas típicas del delito contenido en el art. 576 CP pueden producirse con la intervención de criptoactivos, especialmente atendiendo a la explicación que para cada una de ellas otorga el TS en la STS 279/2013⁵⁴. Este análisis aplicado obedece al hecho de que el principio de taxatividad y la necesidad de precisión en la técnica legislativa elegida en el precepto mencionado son cuestionables, dado el empleo de fórmulas tan amplias y conceptos que parecen solaparse o resultar innecesarios⁵⁵.

3.1. Recabar

Esta conducta típica no se menciona en el delito de blanqueo de capitales, por lo que no se puede partir de la citada referencia jurisprudencial. Por tanto, se puede acudir al sentido etimológico y literal del término. La RAE⁵⁶ define “recabar” como “alcanzar, conseguir con instancias o súplicas lo que se desea”; también como sinónimo de recoger, recaudar y guardar. En lo relativo al delito que se analiza, esta descripción comportamental engloba todo acto realizado por un sujeto o grupo de individuos con el fin de obtener o recolectar fondos, es decir, una búsqueda activa de recursos. Es así como esta conducta tiene una connotación más amplia —e incluso de carácter previo— que la adquisición de fondos.

3.1.1. Financiación colectiva o crowdfunding

Los terroristas pueden recabar o recaudar fondos a través del *crowdfunding* cripto, que se trata de un mecanismo de financiación par-

⁵³ E. ESCUCHURI & M. RUEDA MARTÍN. “Delitos contra el orden público II. Organizaciones y grupos criminales. Organizaciones y grupos terroristas y los delitos de terrorismo”. *Derecho Penal, Parte Especial*. Carlos Romeo y Miguel Ángel Boldova (coords.). Editorial Comares, 2^a ed, 2022, pág. 859.

⁵⁴ Aunque dicha resolución hace referencia al delito de blanqueo de capitales, se entiende explicada la remisión y paralelismo comportamental por las razones ya comentadas. M. OLMEDO CARDENETE. “Delitos contra el orden público (VI): De las organizaciones y grupos terroristas. Delitos de terrorismo”. *Sistema de Derecho penal. Parte especial*. Lorenzo Morillas Cueva (dir.), 2024, págs. 1666 y 1667; hace lo mismo en su obra. Asimismo, J. ZARAGOZA AGUADO. “Artículo 576”. *Comentarios Prácticos al Código Penal*, tomo VI. Manuel Gómez (dir.), Aranzadi, 2015, pág. 664; entiende que la actual descripción de la conducta típica del delito de financiación del terrorismo hace que le sea aplicable toda la casuística jurisprudencial del delito de blanqueo de capitales pues con las últimas reformas se ha producido una coincidencia en los verbos que integran aquella.

⁵⁵ J. GONZÁLEZ CUSSAC & C. VIDALES RODRÍGUEZ. “El nuevo delito de financiación del terrorismo: Consideraciones acerca de su necesidad y conveniencia”. *Op. Cit.*, pág. 186.

⁵⁶ REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española* (23^a Edición), 2014. Consultese en el siguiente enlace: <https://dle.rae.es/recabar>.

ticipativa que se realiza a través de plataformas en línea⁵⁷, por lo que los proyectos que se presentan han de tener claridad y seguridad jurídica⁵⁸. Por eso, ARMOUR y ENRIQUES⁵⁹ consideran que dichas propuestas están fuertemente vinculadas a su buena reputación. Evidentemente esta opción permite a los promotores e inversores de un proyecto interactuar sin necesidad de intermediación bancaria o de empresas de capital de riesgo; constituyendo una alternativa a las formas de financiación tradicional. Esto puede suponer grandes beneficios para el mercado⁶⁰. No obstante, por su alcance, al tratarse de una modalidad de financiación en masa, debe estar muy bien delimitado jurídicamente⁶¹.

Ciertamente, la Autoridad Europea de Valores y Mercados (ESMA, por sus siglas en inglés) ha advertido que las normas europeas sobre servicios financieros no se diseñaron pensando en el *crowdfunding*, por ser un esquema novedoso. Sin embargo, reconoce que las actividades principales de las plataformas que se dedican a ellos quedan sujetas a la II Directiva de Mercados de Instrumentos Financieros⁶². Entre otras cosas, dichas plataformas deben cumplir con tasados requisitos, someterse a un proceso de inscripción, declarar el ámbito de su actividad, cumplir con criterios de reconocida honorabilidad, capacidades y conocimiento suficientes⁶³. Esto será aplicable también al cripto *crowdfunding*, lo cual no solo protege a los inversores sino que permite identificar a los prestadores

⁵⁷ Puede tratarse de cualquier infraestructura digital que facilite la interacción de diversos agentes. Por ejemplo, Y. BOM CAMARGO. "El Crowdfunding, una nueva oportunidad de financiamiento en América Latina y en el Caribe". *Opción*, año 34, núm. 18, 2018, pág. 584; señala a las aplicaciones móviles o páginas web.

⁵⁸ F. ZUNZUNEGUI. "Encuadre sistemático y conceptual de la financiación participativa (Crowdfunding)". *Aspectos legales de la financiación en masa o crowdfunding*". Editorial Tirant Lo Blanch. Matilde Cuena (dir), 2020, págs. 40 y 41.

⁵⁹ J. ARMOUR & L. ENRIQUES. "Individual investors' Access to Crowdfunding: Two regulatory models". *The Economics of Crowdfunding*, 2018, pág. 263.

⁶⁰ Varias de tales beneficios pueden extraerse del trabajo de X. MOLINA; L. MARTÍNEZ & V. DEL CORTE. "Análisis del fenómeno del crowdfunding. El caso de la Plataforma Verkami". *Economía Industrial*, núm. 402, 2016, págs. 73 y 74. A saber, no depende de fuentes tradicionales de financiación, brindando dinamismo al mercado; se reducen los costos de transacción a través de Internet; resulta atractivo para nuevos inversores; propicia el crecimiento del negocio financiero de que se trate; sirve para financiar cualquier tipo de actividad; se gestiona a partir de una cooperación colectiva.

⁶¹ Por sus riesgos, el *crowdfunding* basado en acciones está prohibido en muchos países. *Vid.* A. MORITZ & J. BLOCK. "Crowdfunding: A Literature Review and Research Directions". *Crowdfunding in Europe. State of the Art in Theory and Practice*. FGF Studies in Small Business and Entrepreneurship, Springer. Dennis Brüntje y Oliver Gajda (edit.), 2016, pág. 34.

⁶² ESMA. *Advice Investment-based crowdfunding*, 2014, págs. 2 y 40. Recurso electrónico recuperado del siguiente enlace: https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1560_advice_on_investment-based_crowdfunding.pdf. Consultado por última vez el día 10 de julio de 2025.

⁶³ M. LISSOWSKA. "La regulación europea del crowdfunding: situación actual y desarrollos recientes". *Aspectos legales de la financiación en masa o crowdfunding*". Editorial Tirant Lo Blanch. Matilde Cuena (dir), 2020, pág. 109.

de servicio de plataformas de financiación colectiva y filtrar su participación si no cumplen los requisitos. Todo esto puede apreciarse con detalle en el Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas que, ya en su Considerando 32 advierte cómo los servicios de financiación participativa pueden estar expuestos a riesgos terroristas. Por eso, expone la posibilidad de que, respetando los principios de necesidad y proporcionalidad, los proveedores de servicios de financiación participativa también pasen a formar parte de la lista de entidades obligadas por la Directiva (UE) 2015/849.

En cuanto a lo mencionado en el párrafo anterior, si los terroristas utilizan “empresas fantasma” o empresas legales colaboradoras para que intermedien el *crowdfunding*, estas podrían cumplir formalmente los requisitos establecidos y eludir los controles al ocultar sus verdaderos fines. De hecho, la utilización de entramados empresariales creados para ofrecer actividades aparentemente legales es una de las formas tradicionales de financiación del terrorismo⁶⁴. Dependiendo de la empresa que se trate y a la lícita constitución de la misma, se trataría de una fuente legal de financiación⁶⁵. Es decir, estos fondos pueden ser inicialmente lícitos, ya que pueden ser generados a partir de actividades comerciales legales realizadas por las empresas en cuestión. Y, como se ha querido destacar, el uso de entradas legales para el financiamiento del terrorismo ha sido una táctica recurrente a lo largo de la historia, lo que no variaría en demasía aún si se tratase de proveedores de servicios de *crowdfunding* con tecnología cripto.

Se trata de una transformación de formas de financiamiento terrorista conocidas, a través de plataformas formales de financiación colectiva, las cuales tienen “el potencial de ofrecer nuevas formas de movilizar y recaudar fondos”⁶⁶. Cuando intervienen empresas legalmente constitui-

⁶⁴ M. ANTÚÑEZ. *La financiación del terrorismo internacional y su incidencia en la seguridad y la defensa*. Editor Ministerio de Defensa. Secretaría General Técnica, 2024, pág. 105. En la misma línea, G. SÁNCHEZ MEDERO. “Las fuentes de financiación legales e ilegales de los grupos terroristas”. *Revista Política y Estrategia*, núm. 112, 2008, pág. 52. Asimismo, el GAFI ha reconocido que “el uso de [...] terceros intermediarios, empresas fantasma y otras estructuras corporativas complejas en transacciones también representa importantes vulnerabilidades de financiamiento ilícito”. GAFI. Lavado de dinero y financiamiento del terrorismo en el mercado del arte y las antigüedades. Reporte, 2023, págs. 5 y 41. De hecho, en el mismo informe ilustra lo expuesto con la Operación Harmakis, donde una organización terrorista se valía de una red empresarial de antigüedades para financiarse.

⁶⁵ Las actividades terroristas pueden financiarse, estando esto totalmente aceptado en la doctrina jurídica y la comprensión criminológica del fenómeno. Sobre esto, *vid.* C. MALLADA. “Análisis de la gestión financiera y la estructura de las organizaciones terroristas. Los riesgos emergentes de financiación del terrorismo”. *Anuario de Derecho Penal y Ciencias Penales*, fasc. 1, 2021, págs. 445 y ss.

⁶⁶ S. REIMER & M. REDHEAD. “Bit by Bit Impacts of New Technologies on Terrorism Financing Risks”. RUSI Europe y Project Crafft, 2022, pág. 9.

das, podría dar lugar a la responsabilidad penal correspondiente para personas jurídicas, de acuerdo con el régimen de imputación regulado en el Código Penal y muy bien explicado por TORRES FERNÁNDEZ⁶⁷.

Dicho lo anterior, es también posible que el *crowdfunding* no ostente caracteres formales. El ámbito de los activos virtuales es altamente independiente y escasamente —que no potencialmente— supervisado, de forma que los particulares pueden presentar proyectos cripto en plataformas descentralizadas o espacios de intercambio P2P donde los proyectos no están sujetos a las regulaciones tradicionales. Incluso hay estudios que indican que las redes sociales —en especial *Youtube*, *Tik Tok*, *Facebook*, *Twitter* (actual X) e *Instagram*— han resultado útiles para promocionar *crowdfundings* de manera informal, versátil y masiva⁶⁸. Esto permitiría una mayor flexibilidad y anonimato en la promoción y recaudación de fondos, especialmente cuando se busca eludir las normativas tradicionales de control y supervisión. Resulta distintivo del caso anterior, pues al no pasar los filtros legales de las personas jurídicas o físicas profesionales hay menos probabilidades de identificar a las partes y, por ende, prevenir y responder a su comportamiento ilícito.

El GAFI⁶⁹ reconoce que el potencial anonimato es la razón principal por la que los terroristas se valen de las criptomonedas para recaudar fondos a través de plataformas de financiación colectiva. Además, advierte que los terroristas crean nuevas direcciones de activos virtuales, explican a los donantes cómo enviar los fondos cripto de la forma correcta, eligen preferentemente cadenas de bloques de código abierto y usan *mixers*⁷⁰ o intercambian los criptoactivos recibidos a otras billeteras antes de convertirlos en moneda fiduciaria a través de un proveedor de servicios de criptoactivos, o bien usan directamente los criptoactivos si es posible para financiar actividades o compras que atiendan sus necesidades operativas.

⁶⁷ M.E. TORRES FERNÁNDEZ. “La regulación de la responsabilidad penal de las personas jurídicas por delitos de terrorismo. El terrorismo, ¿riesgo en el tráfico jurídico y empresarial?”. *Anuario de Derecho Penal y Ciencias Penales*, tomo 73, fasc. 1, 2020, págs. 160 y ss.

⁶⁸ A. MOHAMAD & A. CHE HUSSIN. “Understanding Crowdfunding via Social Media: A Review of the Relevancy of Previous Studies”. *International Journal of Academic Research in Business and Social Sciences*, vol. 14, núm. 1, 2024, pág. 1132. Asimismo, C. MANGGARANI & Z. AHMAD. “The Determining Factors of Student Intention to Donate in Social Crowdfunding Media”. *Hasanuddin Economics and Business Review*, vol. 4, núm. 1, 2020, pág. 7 y ss; destacan que las redes sociales facilitan la búsqueda de personas con ideas afines al proyecto o supuesto proyecto de financiación ofrecido.

⁶⁹ GAFI, “Crowdfunding for terrorism financing”. Informe, 2023, págs. 27 a 30. Recurso electrónico recuperado del siguiente enlace: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf>. Consultado por última vez el día 10 de julio de 2025.

⁷⁰ Estos servicios intercambian los flujos de muchos propietarios para reducir la transparencia de las transacciones con activos virtuales. Para el GAFI se trata de un área de riesgo a la que se debe dar prioridad, pues ofusca aún más los movimientos y socavan la capacidad de los prestadores de servicios de activos virtuales -sujetos obligados por la normativa antiblanqueo- para implementar medidas de KYC y debida diligencia.

Un caso de interés que refleja la complejidad que puede alcanzar el *crowdfunding* cripto tuvo lugar en 2020, cuando un gran grupo de cómplices, que querían financiar una red yihadista en Siria, compraron “cupones de criptomonedas” en estancos con valor de entre 10 y 150 euros cada uno⁷¹. De acuerdo con un asesor de inteligencia, entrevistado por un medio español especializado, esto constituye una arquitectura que combina diversas entidades y permite a los yihadistas y sus partidarios financieros “explotar varias vulnerabilidades y acumular capas de anonimato”⁷². Comprar estos cupones es posible también por Internet, sin necesidad de presentar ninguna identificación. Además, en este caso los colaboradores utilizaron servicios de mensajería encriptada y los cupones los cifraron, de forma que era muy difícil interceptar esas comunicaciones. La mayoría de los cupones se compraron en Francia, aunque había partidarios en otros países, enviaron fotografías a los terroristas que convocaron la campaña de financiación y se convirtieron a Bitcoin en Turquía, evidenciando los problemas que esto puede tener en lo relativo a la Ley penal en el espacio. Los terroristas a quienes se destinaron los fondos tenían órdenes de detención internacionales por causas terroristas, pero aún así fueron capaces de activar con éxito sus códigos de los cupones⁷³. También se recogieron donaciones presencialmente. Estas transacciones eran tan pequeñas que no saltan las alarmas por transacciones sospechosas, aunque sí por el número cuantioso de ellas. El caso muestra el potencial de las criptomonedas para recaudar fondos descentralizadamente, incluso fuera de las plataformas, mediante llamadas masivas a donar.

Así, las campañas de financiación del terrorismo actuales incluyen técnicas variadas de ofuscamiento que mantienen las bases del *crowdfunding* pero les otorgan una sofisticación notoria con herramientas tecnológicas. Cada vez son más las personas entusiastas de donar sus fondos a través de plataformas de este tipo, especialmente porque los promo-

⁷¹ M. HUILLET. “La policía francesa arresta a una red de financiación del terrorismo que usaba cupones de Bitcoin” [Comunicado de prensa]. Cointelegraph, 30 de septiembre de 2020, s/p. Recurso electrónico recuperado del siguiente enlace: <https://es.cointelegraph.com/news/french-police-arrest-terror-financing-ring-that-used-bitcoin-coupons>. Consultado por última vez el día 10 de julio de 2025.

⁷² G. VEDRENNE. “‘Cupones’ de Criptomonedas Financiaron el Yihadismo Sirio, Afirman Autoridades Francesas” [Comunicado de prensa]. Acams Conexión, 13 de octubre de 2020, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.acamstoday.org/cupones-de-criptomonedas-financiaron-el-yihadismo-sirio-afirman-autoridades-francesas/>. Consultado por última vez el día 10 de julio de 2025.

⁷³ L. FROST. “Terroristas usaron cupones de criptomonedas para enviar dinero de Francia a Siria” [Comunicado de prensa]. Decrypt, 30 de septiembre de 2020, s/p. Recurso electrónico recuperado del siguiente enlace: <https://decrypt.co/es/43402/terroristas-usaron-cupones-de-criptomonedas-para-enviar-dinero-de-francia-a-siria>. Consultado por última vez el día 10 de julio de 2025.

tores pueden apelar a actitudes filantrópicas, comunitarias, patrióticas⁷⁴ y otras con fuerte impacto emocional. Si los inversores desconocen los fines terroristas del proyecto en cuestión evidentemente no deberían ser responsables penalmente. Sin embargo, si se trata de un proyecto con indicios claros o exposición directa de contenido terrorista, podría cuestionarse lo anterior. Por ejemplo, un terrorista o un grupo terrorista podría potencialmente aprovechar el crowdfunding en la *Dark web* para recaudar fondos de manera anónima y eludir las medidas de control que existen en plataformas más convencionales y reguladas. En este supuesto probablemente los terroristas o sus colaboradores no disimularán los objetivos, sino que intentarían simpatizar con ellos, debido a la sensación de impunidad que le producen las técnicas de ofuscación.

3.1.2. Minería de criptomonedas

La minería es un aspecto clave en la generación de nuevas criptomonedas y en la validación de nuevos bloques. Pero como también se ha indicado, esta actividad genera beneficios económicos a los mineros. En la mayoría de los casos, estos sujetos deben configurar sus ordenadores y registrar sus usuarios para convertirse en estos nodos especiales del sistema cripto⁷⁵. En España incluso deben declarar sus ingresos en la declaración de la renta. Y a nivel internacional, es un área donde se está experimentando un mayor proceso regulador, como destaca el Departamento de Seguridad Nacional de los Estados Unidos⁷⁶. Estos factores no interesan en demasía a los terroristas que, sin duda, optan por aquellas técnicas/herramientas que evitan su identificación.

No obstante lo anterior, ciertos datos indican un auge de la minería ilícita de criptomonedas desde 2017⁷⁷. Esta se define por ROMANOV y TUKAEVA como el “desvío no autorizado de electricidad y recursos para minar criptomonedas”⁷⁸. En términos generales, la minería ilícita de cri-

⁷⁴ S. BERNARDINO; J. FREITAS & J. CADIMA. “Social crowdfunding: A new model for financing regional development?”. *Journal of Urban and Regional Analysis*, vol. 8, núm. 2, 2016, pág. 111.

⁷⁵ A. IRWIN & A. TURNER. “Illicit Bitcoin transactions: challenges in getting to the who, what, when and where”. *Journal of Money Laundering Control*, vol. 21, núm. 3, 2018, pág. 299.

⁷⁶ DEPARTAMENTO DE SEGURIDAD NACIONAL DE LOS ESTADOS UNIDOS. “Combatting illicit activity utilizing financial technologies and cryptocurrencies”. Public-Private Analytic Exchange Program, 2022, pág. 36.

⁷⁷ CYBER THREAT ALLIANCE. “The illicit cryptocurrency mining threat”. Informe, 2018, pág. 4. Disponible en el siguiente enlace: <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf>. Consultado por última vez el día 10 de julio de 2025. En el informe se señala un incremento de más del 400% en los últimos años, sin indicios de que vaya a cambiar la tendencia.

⁷⁸ Y. ROMANOV & A. TUKAEVA. “Minería ilegal de criptomonedas: impacto en el comercio y la regulación” [Artículo de prensa]. Crypto Robotics, 10 de enero de 2025,

tomonedas puede producirse utilizando la técnica del *cryptojacking* o un *malware* de minería de criptomonedas basado en binarios, en el cual se incrusta el proceso de minería⁷⁹. También existe la posibilidad de que se minen criptomonedas en la nube, alquilando potencias de cálculo en centros de dato, sin necesidad de adquirir *hardware* potente y especializado. En este último caso, los delincuentes preferirían solicitar estos servicios de formas clandestinas, para así difuminar el rastreo, incluso pudiendo solicitar el uso y explotación de la billetera de un tercero colaborador, utilizando cuentas o identidades robadas, pagando el servicio con criptomonedas para dificultar la identificación de quien paga el servicio, aprovechar máquinas comprometidas o secuestradas⁸⁰, entre otros métodos.

ELLIPTIC⁸¹ ha emitido un estudio donde refleja que Irán ha financiando las actividades de grupos terroristas islamistas, como son Hezbolá y Hamás, con la minería. Este país del Oriente medio legalizó tal actividad en 2019 y la realidad práctica indica que su uso no ha dejado de crecer⁸², lo que ha facilitado también la recaudación de fondos por esta vía desde instancias estatales para financiar determinadas causas. Ejemplo de ello

s/p. Recurso electrónico recuperado del siguiente enlace: <https://cryptorobotics.ai/es/news/illegal-crypto-mining-impact-trading-regulation/>. Consultado por última vez el día 10 de julio de 2025. Los daños de la minería ilegal no son solo de carácter delictivo sino también medioambiental. En ocasiones esta se practica con conexiones remotas a equipos ubicados en casas abandonadas, con alto riesgo de incendio. Por ejemplo, puede consultarse THE NATION. “Illegal crypto mining machines seized from abandoned houses” [Comunicado de prensa]. 15 de marzo de 2025, s/p. Recurso electrónico recuperado del siguiente enlace web: <https://www.nationthailand.com/news/general/40047447>. Consultado por última vez el día 10 de julio de 2025.

⁷⁹ S. PASTRANA & G. SUAREZ-TANGIL. “A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth”. En *IMC '19: Proceedings of the Internet Measurement Conference*, 2019, pág. 73. En el trabajo de los autores se señala que los beneficios obtenidos con esta clase de minería alcanzan los de una granja dedicada a este proceso computacional.

⁸⁰ Por ejemplo, pueden valerse de los llamados *botnets*, abordados por el INCIBE. Este organismo los define como “un conjunto de ordenadores, denominados *bots*, infectados con un tipo de *malware* que son controlados remotamente por un atacante y que pueden ser utilizados de manera conjunta para realizar actividades maliciosas”. Para evitar esto, INCIBE pone a disposición de los residentes en España el servicio AntiBotnet, para identificar si un dispositivo personal con conexión a Internet han sido relacionados con estos bots u otras amenazas relacionadas. Además, ofrece enlace a herramientas que permiten desinfectar el equipo. Para más información, pueden consultarse los siguientes enlaces web: <https://www.incibe.es/aprendeciberseguridad/botnet> y <https://www.incibe.es/ciudadania/herramientas/servicio-antibotnet>. La minería con botnets es un uso ilícito vinculado a Zcash. *Vid.* C. DION-SCHWARZ; D. MANHEIM & P. JOHNSTON. *Terrorist Use of Cryptocurrencies*, National Security Research Division, 2019, pág. 50.

⁸¹ ELLIPTIC. “How terrorist groups are exploiting crypto to raise funds and evade detection”. Reporte, 17 de Agosto de 2023, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection>. Consultado por última vez el día 10 de julio de 2025.

⁸² I. REZAEINEJAD. “Challenges and opportunities cryptocurrency in Iran economy & e-businesses”. *RUDN Journal of Economics*, vol. 29, núm. 4, 2021, pág. 689.

es que, en los cinco años posteriores a la legalización de la minería, ha recabado millones de dólares a través de esta técnica para comprar importaciones, transferir fondos y financiar diversas organizaciones terroristas. Así lo ha precisado el Senado de los EEUU, inquiriendo al Gobierno respuestas efectivas, ya que tales comportamientos ponen en riesgo la seguridad del país americano y del mundo⁸³.

En caso de que los terroristas requieran del apoyo de colaboradores que les suministren cuentas ajenas o equipos remotos o físicos para minar, los segundos deberían responder como cooperadores necesarios del delito de financiación del terrorismo. De acuerdo con el art. 28 CP, son aquellos que colaboran a la ejecución del mismo con un acto sin el cual no se habría efectuado, por lo que se consideran a efectos penológicos como autores. Si la financiación depende del soporte y ayuda de terceros, estaríamos ante esta forma de participación delictiva. Ahora bien, identificar casos de minería ilegal no es sencillo y, más aún, es imposible solo con la intervención del Derecho. Pero el trabajo de RUSSO, ŠRNDIĆ y LASKOV⁸⁴ propone el uso de un detector de minería ilícita basado en tecnologías de aprendizaje automático que reconstruye y sofistica protocolos usados en modelos anteriores. El entrenamiento de la máquina se realiza solo consultando el tráfico de minería sin conexión, por lo que no ocasiona problemas para la privacidad. Y, en la fase de prueba, el experimento alcanzó una tasa de éxito del 98,94% de aciertos, demostrando ser confiable y robusto frente a técnicas de ofuscación. También hay escáneres avanzados para mitigar el *cryptojacking* en determinadas plataformas, como el *Cijitter* propuesto por LI et.al.⁸⁵, que permite incluso que el minero ilícito no pueda obtener ganancias por su acto, evitando la rentabilidad del delito.

3.2. Adquirir

De acuerdo con la STS 279/2013, citada en lo que precede, la adquisición ha de entenderse como la incorporación de bienes al patrimonio

⁸³ Puede consultarse en el siguiente enlace web: <https://www.warren.senate.gov/imo/media/doc/2024.05.01%20Letter%20to%20Treasury,%20White%20House,%20DoD%20on%20Iran%20Cryptomining.pdf>.

⁸⁴ RUSSO, ŠRNDIĆ y LASKOV. "Detection of illicit cryptomining using network metadata". *EURASIP Journal on Information Security*, núm. 1, 2021, págs. 7, 13 y 16. Los autores explican que los mineros ilícitos suelen operar en *pools*, o piscinas, de minería. Es decir, varios mineros se agrupan para combinar poder computacional para minar bloques de criptomonedas. Normalmente, las operaciones maliciosas de minería se realizan en piscinas públicas legítimas, por lo que tales actores se ven obligados a usar los mismos clientes e implementaciones y por eso es posible analizar sus operaciones.

⁸⁵ Z. LI; et.al. "Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms". *IEEE Symposium on Security and Privacy (SP)*, 2022, pág. 9.

propio, bien sea a título oneroso o gratuito. En el primer caso, el adquirente recibe de los terroristas o quienes colaboran económicamente con ellos un producto, bien o servicio a cambio de fondos que se dirigirán a objetivos terroristas. En el segundo, la adquisición por parte de estos sujetos no exige un intercambio, sino que suele presentarse como una donación⁸⁶. Tanto en esta conducta como en la precedente queda claro que el legislador castiga la aportación de fondos terroristas sin importar el medio empleado, independientemente de que se produzca de forma directa o indirecta⁸⁷. En este sentido, hay que recordar que los bienes o fondos utilizados con fines terroristas no siempre son ilegítimos, ni siempre requieren un blanqueo previo. En ocasiones son el producto de actos lícitos, que se convierten en objeto delictivo *a posteriori*, cuando son dirigidos a tales proyectos criminosos⁸⁸.

3.2.1. Venta de productos y servicios en la *Dark Web*⁸⁹

Es ampliamente admitido que los terroristas utilizan la Internet profunda para recaudar fondos y realizar transacciones financieras con criptomonedas, con el objeto de evitar la interferencia y los controles que naturalmente imponen los reguladores financieros⁹⁰. De esta manera, esta porción de la web no solo les permite lanzar campañas y propuestas para recaudar los fondos, sino ofrecer productos y servicios ilícitos para adquirir fondos a cambio de una contraprestación. Es decir, se trata de un

⁸⁶ Siguiendo a la doctrina de los países del entorno, no basta con la mera intención de las partes para distinguir la adquisición onerosa de la gratuita, sino que es necesario un elemento objetivo: la contraprestación, obligación, prestación o sacrificio que se suministra a cambio. Al respecto, *vid.* J. PRADA GONZÁLEZ. “La onerosidad y gratuitad de los actos jurídicos”. *Anales de la Academia Matritense del Notariado*, tomo 16, 1968, págs. 200 y 201.

⁸⁷ J. GONZÁLEZ CUSSAC & C. VIDALES RODRÍGUEZ. “El nuevo delito de financiación del terrorismo: Consideraciones acerca de su necesidad y conveniencia”. *Op. Cit.*, pág. 185.

⁸⁸ F. NAVARRO CARDOSO. “El delito de financiación del terrorismo en el Código Penal español (art. 576)”. *Financiación del terrorismo*. Juan Carlos Ferré y Ana Pérez Cepeda (dirs.). Editorial Tirant Lo Blanch, 2018, págs. 87 y 88.

⁸⁹ En la obra de L. GARCÍA SIGMAN. “Narcotráfico en la Darkweb: los criptomercados”. *URVIO Revista Latinoamericana de Estudios de Seguridad*, núm. 21, 2017, pág. 193; las características de los llamados “criptomercados” (mercados de la Dark Web que usan criptoactivos) son las siguientes: se ofertan productos, los usuarios pueden elegir y comparar tales ofertas, tienen un aspecto estructural y funcional a los mercados lícitos de *e-commerce* y cuentan con distintas estrategias y tecnologías para ocultar la identidad de los participantes.

⁹⁰ N. MALIK. *Terror in the dark. How terrorists use encryption, the Darknet, and Cryptocurrencies*. The Henry Jackson Society, 2018, pág. 4. Las organizaciones terroristas pueden ejecutar el *ransomware* con la compra de *software*, la reutilización de código fuente filtrado o la conversión de afiliados. Al respecto, *vid.* DEPARTAMENTO DE SEGURIDAD NACIONAL DE LOS ESTADOS UNIDOS. “Ransomware Attacks on Critical Infrastructure Sectors”. Public-Private Analytic Exchange Program, 2022, pág. 22.

espacio cibernetico de dialogo, coordinación y acción de actividades ilegales⁹¹; siendo especialmente útil para el terrorismo, que es un fenómeno polisémico que requiere de particular precisión en todas estas fases. El auge de las criptomonedas ha hecho que la mayoría de los mercados de la red oscura las manejen como medio económico transaccional. Hay estudios que indican que se usan en un 80%, frente al 20% que conforman las transferencias de dinero o el pago en efectivo⁹². Este entorno cibernetico se ha convertido en una herramienta poderosa para grupos terroristas, que pueden explotar las ventajas de la *Dark web* y las criptomonedas para financiar sus actividades de forma más difusa en términos de trazabilidad en comparación con métodos ordinarios. Especialmente, se aprecia una prevalencia de estos activos virtuales para pagar sustancias ilícitas en la Internet profunda no indexada⁹³.

La anécdota clara de lo expuesto antes es *Silk Road*; un mercado negro *online* que operaba en un sitio web de la red TOR. Ross Ulbricht, un precursor del criptoanarquismo, se consideró el padre de dicho mercado. En él se ofrecían principalmente drogas, pasaportes falsos y mercancía de contrabando; normalmente a cambio de Bitcoin⁹⁴. La distribución de estos productos ilícitos implica diversas etapas que, a su vez, implican múltiples delitos. *Silk Road* garantizaba el anonimato de los vendedores y los compradores, que se encontraban en un espacio muy similar al de Amazon, eBay y otros conocidos. De acuerdo con CHRISTIN⁹⁵, para acceder al susodicho mercado era necesario instalar TOR o un proxy web que permitiera conectarse a la red, crear una cuenta —para lo que solo era necesario aportar un nombre de usuario, contraseña y un PIN para hacer retiros—, respetar las normas de uso —que únicamente prohibían los fraudes y cualquier material relacionado con la pedofilia, sin restringir otros delitos—, realizar un pedido y esperar recibirla en una dirección física. La propia plataforma recomendaba suministrar una dirección

⁹¹ N. ROSALINE & O. NYAMWAYA. “The Dark Web and Cryptocurrencies: A ‘trust’ dilemma for digital commerce?”. *Baraton Interdisciplinary Research Journal*, núm. 8, 2018, pág. 5.

⁹² C. JORDÁ; C. PÍRIZ & A. GIMÉNEZ-SALINAS. “Los criptomercados ilícitos de tráfico de drogas en la DarkWeb: un estudio exploratorio empírico”. *Revista Española de Investigación Criminológica*, vol. 22, núm. 2, 2024, pág. 16.

⁹³ D. GOLDBARSHT. “Dancing in the Dark: Terrorist Financing Via the Dark Web”. *Financial Crime and the Law*, Doron Goldbarsht y Louis de Koker (eds.). Springer, 2024, pág. 183.

⁹⁴ Resalta P. SALDAÑA TABOADA. “Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes”. [Tesis de doctorado no publicada]. Universidad de Granada, 2023, pág. 50; que la utilización de Bitcoin en *Silk Road* fue uno de los eventos que elevó la popularidad de la criptomoneda. Esto demuestra que el auge de los criptoactivos está condicionado a factores emocionales de muy diversa índole, y que incluso sus vulnerabilidades delictivas han jugado un papel importante en su expansión.

⁹⁵ N. CHRISTIN. “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace”. *22nd International Conference*, s/n, 2013, pág. 2.

distinta a la del domicilio del usuario. *Silk Road* estuvo operativo poco tiempo hasta que fue desmantelada por el FBI⁹⁶ y arrestaron a su creador. En este espacio había tres rasgos predominantes: coordinación, cohesión social y tendencia extremista⁹⁷; lo que conforma un caldo de cultivo para que los terroristas o personas vinculadas con ellos pudieran aprovechar de vender allí productos ilícitos con los que financiar sus actividades⁹⁸.

El caso anterior no hace referencia a una plataforma específicamente dedicada al terrorismo, aunque potencialmente explotable por sus actores. Sin embargo, sí lo es la red delictiva desmantelada por la Operación Jenner, en la que intervino la Jefatura Superior de Madrid de la Policía Nacional española. Dicha organización criminal compleja, en la que participaron terroristas extremistas islámicos, ofrecía pasaportes de vacunación COVID falsos a cambio de, preferentemente, criptomonedas⁹⁹. La oferta de este servicio ilegal se realizaba en grupos de mensajería instantánea de carácter negacionista a cambio de precios fijos de entre cincuenta y más de mil euros, dependiendo del tipo de documento solicitado y el momento en que lo pidiese. Para determinar si las actividades de la red tienen alcance en España, agentes especializados en ciberpatrullaje tuvieron que infiltrarse en la *Dark Web* —donde podían consultarse los anuncios de los mencionados documentos falsos— y hacerse pasar por simpatizantes del islamismo radical y justificar con base a sus propias creencias que no podían ir a Francia¹⁰⁰ a recoger los pasaportes. Los salafistas les contestaron que tenían colaboradores en España, quienes podrían hacer la entrega¹⁰¹. Este complejo diseño estructural con fines

⁹⁶ S. BARÓN QUINTERO. “Los delitos realizados mediante la Dark Net”. *Revista Penal México*, núm. 23, 2023, pág. 179.

⁹⁷ B. LOBERT JONES. “The 21st Century DarkNet Market: Lessons from the Fall of Silk Road”. *International Journal of Cyber Criminology*, vol. 10, núm. 1, 2016, pág. 44.

⁹⁸ L. TRAUTMAN. “Virtual currencies; Bitcoin & What now after Liberty Reserve, Silk Road, and Mt. Gox?”. *Richmond Journal of Law & Technology*, vol. 20, núm. 4, 2014, pág. 12; recuerda que el narcotráfico tiene una estrecha relación con grupos terroristas internacionales. *Cfr.* J. MARTIN. “Lost on the Silk Road: Online drug distribution and the ‘cryptomarket’”. *Criminology & Criminal Justice*, vol. 14, núm. 3, 2013, s/p; quien considera que no es fácil establecer el vínculo entre la venta de drogas ilícitas y el crimen organizado en el caso de *Silk Road*. Versión electrónica disponible en el siguiente enlace: https://journals.sagepub.com/doi/full/10.1177/1748895813505234?casa_token=bkQiSjN2QrAAAAAA%3A51bMAB4Kpr6Lm3FeNqJ2654gyg4oOMpATeQyTeNdwWowCr6UNSHtkDL2VcK6cSYfYGPIdGK2p2JjNA.

⁹⁹ A. TERRADILLOS. “La red de pasaportes COVID falsos cobraba en criptomonedas desde cuentas abiertas en el Campo de Gibraltar y Lituania” [Comunicado de Prensa]. Cadena Ser, 28 de enero de 2022, s/p. Recurso electrónico recuperado del siguiente enlace web: <https://cadenaser.com/2022/01/28/la-red-de-pasaportes-covid-falsos-cobraba-en-criptomonedas-desde-cuentas-abiertas-en-el-campo-de-gibraltar-y-lituania/>. Consultado por última vez el día 10 de julio de 2025.

¹⁰⁰ La red criminal operaba en Francia, Lituania, Gibraltar, España y otros.

¹⁰¹ ONDACERO. “Territorio Negro: Los camaleones de la Policía y los falsos vacunados de Covid” [Comunicado de Prensa], 31 de mayo de 2022, s/p. Recurso electrónico recuperado del siguiente enlace web: <https://www.ondacero.es/programas/julia-en-la-onda/audios->

delictivos no fue imposible de rastrear, esta vez siguiendo un sistema de investigación más tradicional (agentes encubiertos), aunque usando tecnologías para comunicarse a distancia a través de la red oscura. Aunque detrás de esta red no solo habían terroristas, sino también traficantes de drogas y otros, en este punto se hará hincapié en el primero.

La emisión y oferta de pasaportes falsos de vacunación o pruebas negativas de COVID es una conducta perfectamente subsumible por la tipificación del delito de financiación del terrorismo. No solo cumple el tipo básico del apdo. 1 del art. 576 CP, sino que daría lugar a la agravación específica del apdo. 3: “En el caso de que la conducta a que se refiere el apartado 1 se hubiera llevado a cabo [...] cometiendo [...] falsedad documental (como los pasaportes de vacunación falsos o PCR) o mediante la comisión de cualquier otro delito, éstos se castigarán con la pena superior en grado a la que les corresponda, sin perjuicio de imponer además la que proceda conforme a los apartados anteriores”. Es lo que se conoce por NAVARRO CARDOSO¹⁰² como uno de los supuestos mediales, es decir, donde se comete un delito para cometer el de financiación, para lo cual opina que aplica la solución de un concurso real y no de uno medial. No obstante, la falsedad documental también es uno de los delitos mencionados en la definición de terrorismo ofrecida por el art. 573.1 CP, por lo que habría que aplicar el principio de alternatividad para no incurrir en una concurrencia del *non bis in idem*¹⁰³.

Otro ejemplo de la relación entre la *Dark web* y las criptomonedas para la financiación del terrorismo se aprecia en la SAN 21/2023¹⁰⁴, por la que se condena por pertenencia a organización terrorista¹⁰⁵ a unos individuos que se movilizaron a occidente para expandir los ideales islámicos. Para financiar sus actividades terroristas, los individuos realizaron actividades financieras fraudulentas. Uno de ellos obtenía datos financieros robados disponibles en la *Dark Web* y pagaba con criptomonedas. Los demás convertían a estos activos los beneficios obtenidos de otras formas delictivas, como el *carding*. La compra y venta de criptomonedas obtenidas ilícitamente fue apreciada por las autoridades con el análisis de los dispositivos electrónicos de los acusados.

3.2.2. Diseño y venta de NFTs

podcast/territorios/negro/territorio-negro-camaleones-policia-falsos-vacunados-covid_202205316296346ed7b96e0001f87560.html. Consultado por última vez el día 10 de julio de 2025.

¹⁰² F. NAVARRO CARDOSO. “Los tipos dolosos del delito de financiación del terrorismo”. *Op. Cit.*, pág. 21.

¹⁰³ J. MORCILLO JIMÉNEZ. “Delitos contra el orden público”. *Op. Cit.*

¹⁰⁴ SAN 21/2023, de 3 de octubre de 2023.

¹⁰⁵ La resolución judicial fue recurrida en apelación y la Sección de Apelación de la Sala de lo Penal de la Audiencia Nacional les absolvio por este delito y les condenó por colaboración con organización terrorista en la SAN 1/2024, de 9 de enero de 2024.

El terrorismo moderno se caracteriza por estar muy bien provisto a nivel logístico¹⁰⁶, incluyendo hoy en día su robusto nivel de digitalización. En 2022 se conoció el primer NFT creado por un simpatizante terrorista, gracias a una publicación del periódico *The Wall Street Journal*. El artículo lo describía como “una simple tarjeta digital que elogia a militantes islamistas por un ataque a una posición talibán en Afganistán”¹⁰⁷. El *token* fue descubierto por un investigador estadounidense y otros agentes de inteligencia descubrieron que el mismo usuario creó dos NFT más, ambos vinculados igualmente con ideales terroristas¹⁰⁸. Más allá de la financiación, sobre la que se hablará inmediatamente después, lo que se demuestra con este caso es una combinación de dos aspectos clave:

- Los terroristas se están tecnificando en un grado sustancial: Crear un NFT es una tarea mucho más avanzada que solo intercambiar criptomonedas. Demuestra un conocimiento más avanzado sobre blockchain, los activos virtuales en generales y otras tecnologías digitales relacionadas con este ecosistema¹⁰⁹. Así, el aprovechamiento que estos actores hacen de las herramientas de la era digital ya no es una mera adaptación o adquisición de conocimiento básico, sino una comprensión avanzada de las mismas, que exige el mismo nivel de atención y tecnicismo de los agentes de las Fuerzas y Cuerpos de Seguridad de los Estados.
- Los terroristas utilizan medios financieros no solo por objetivos económicos, sino para ganar visibilidad y crear una imagen sofisticada: Los NFT, al ser una forma relativamente nueva y avanzada de interacción con el mundo digital, pueden servir como un medio de publicidad que da una imagen moderna y atractiva¹¹⁰. Esto es es-

¹⁰⁶ J. MONTERO GUERRA. “Análisis psicológico del terrorismo”. *Anuario de Psicología Jurídica*, vol. 7, núm. 1, 1997, s/p. Recuperado de la versión electrónica disponible en el siguiente enlace: <https://journals.copmadril.org/api/art/84438b7aae55a0638073ef798e50b4ef>. Consultado por última vez el día 13 de abril de 2025.

¹⁰⁷ I. TALLEY. “Islamic State Turns to NFTs to Spread Terror Message” [Comunicado de Prensa]. *The Wall Street Journal*, 6 de septiembre de 2022, s/n. Recurso electrónico recuperado del siguiente enlace web: <https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800>. Consultado por última vez el día 10 de julio de 2025.

¹⁰⁸ S. KATTE. “Los grupos terroristas podrían recurrir a los NFT para recaudar fondos y difundir mensajes” [Artículo de prensa]. *Cointelegraph*, 05 de septiembre de 2022, s/p. Recurso electrónico recuperado del siguiente enlace web: <https://es.cointelegraph.com/news/terror-groups-may-turn-to-nfts-to-raise-funds-and-spread-messages-wsj>. Consultado por última vez el día 10 de julio de 2025.

¹⁰⁹ Puede consultarse la complejidad de este proceso creativo y técnico en T. LAURENCE & S. KIM. “Developing Your Knowledge: A Step-by-Step Guide to Programming Your Own NFT”. *NFTs For Dummies*. 1^a Edición, Editorial Wiley, 2021, pág. 83 y ss. También en M. FORTNOW & Q. TERRY. *The NFT Handbook. How to create, sell and buy non-fungible tokens*. 1^a Edición, Editorial Wiley, 2022, pág. 125 y ss.

¹¹⁰ Como mencionan P. REY; P. RIVAS & O. SÁNCHEZ. “Propaganda, radicalismo y terrorismo: la imagen del Daesh”. *Estudios sobre el mensaje periodístico*, núm. 23, 2017,

pecialmente sabido en el caso de los jóvenes, que suelen estar más involucrados en novedades de este tipo¹¹¹. Este vehículo simbólico para sus mensajes, hacen que los terroristas puedan generar mayor notoriedad y resonar en comunidades a las que antes no llegaban con tanta fuerza.

El hecho de que los NFTs sean códigos informáticos únicos registrados en la cadena de bloques, los sitúa como piezas digitales únicas que, en muchos casos, pueden alcanzar mucho valor económico. Por eso no son intercambiables, pero sí tienen mucho potencial para ser vendidos¹¹², lo que repercutiría en un rédito económico para la parte vendedora. Así pues, podrían ser un instrumento pertinente para adquirir fondos terroristas, incluso creando una imagen engañosa del valor del activo, creando una apariencia de legitimidad¹¹³ o potenciando sentires radicales. Aunque la utilización de NFTs con fines terroristas es aún incierta y hacen falta más trabajos especializados al respecto, los escasos datos que se tienen demuestran que es un área a la que dar atención. Las razones por las que los terroristas pueden optar por negociar con NFTs para obtener fondos con los que financiar sus actividades operativas y cubrir sus necesidades estructurales son señaladas por GESLEVHI y VOLOVELSKY¹¹⁴: el anonimato y pseudoanonimato de los NFT, la facilidad de transferencia y alcance global, la insuficiente y poco coordinada regulación y supervisión, la capacidad para hacer transferencias de valor en las redes que conforman un grupo u organización terrorista y la dificultad de verificación de la procedencia del bien digital. Es rotundamente coincidente con las características de las criptomonedas.

La venta de NFT para obtener ganancias que se destinarán a objetivos terroristas es una conducta subsumible en el tipo penal del art. 576 CP. No obstante, el problema palmario es que la gran mayoría de los merca-

pág. 210; “el hecho de que un grupo terrorista utilice a la opinión pública a su favor no sólo no es nuevo, sino que es la propia esencia del terrorismo”.

¹¹¹ Esta idea puede apreciarse con profundidad en el trabajo de J. SILALAHI; T. BUCHARA. & S. HENDRATNO. “Young Generation Point of View About Non-Fungible Token as a Future Currency and Assets”. *E3S Web of Conferences*, núm. 426, 2023.

¹¹² A. MOOIJ. *Regulating the Metaverse Economy. How to Prevent Money Laundering and the Financing of Terrorism*. Springer, 2023, pág. 104.

¹¹³ I. FETSYAK. “Consideraciones sobre la prevención del blanqueo de capitales y financiación del terrorismo mediante los tokens no fungibles (NFT)”. *REDUR*, núm. 20, 2022, págs. 96 y 97.

¹¹⁴ N. GESLEVICH & U. VOLLOVELSKY. “Digital assets, anti-money laundering and counter financing of terrorism: An analysis of evolving regulations and enforcement in the era of NFTs”. *The Cambridge Handbook on Law and Policy for NFTs*, Forthcoming, 2023, págs. 19 y 20. Otras razones indicadas por E. OGUZ; N. BASAK & A. KAPUSUZOGLU. “The use of crypto coins to finance terrorism”. *Economic Science*, vol. 20, 2021, pág. 16; son: deficiencias en procedimientos de seguridad, baja tributación, falta de un mecanismo de control efectivo y ausencia de restricciones en la fijación de precios y la comercialización en el mercado de los NFTs.

dos de NFT no imponen procesos de KYC o medidas anti blanqueo o de lucha contra la financiación del terrorismo¹¹⁵. Por sus especificaciones técnicas estos *tokens* no suelen estar incluidos en las regulaciones que se dictan de criptoactivos, por lo que es más notoria su situación de alegalidad. Sin embargo, los proveedores de servicios de criptoactivos sí pueden aplicar algunos de estos métodos profilácticos en el momento en que esos NFT se intercambien por criptomonedas u otros criptoactivos; aunque no debe considerarse la solución definitiva.

3.2.3. Financiación estatal

Se puede distinguir entre la financiación obtenida por los propios terroristas o grupos privados de apoyo de aquella suministrada por el Estado. De acuerdo con HINOJOSA¹¹⁶, dentro de la segunda alternativa se diferencia también el caso de que el propio Estado sea quien comete o planifica el acto terrorista y cuando es quien financia actividades terroristas realizadas por terceros. Sin embargo, no siempre el acto financiador tiene carácter internacional, puesto que es frecuente en el terrorismo interno¹¹⁷. La financiación del terrorismo estatal mediante criptomonedas es un tema complejo y, aunque no es algo ampliamente documentado, hay indicios de que es una realidad práctica. Entre otros factores, en casos de este tipo es prevalente la llamada “cifra dorada”¹¹⁸. Por tanto, analizar este punto implica esa limitación que le es inherente.

Para mantener un orden lógico y esquemático ya se ha hecho referencia al apoyo de Irán a Hamás con la minería de criptomonedas. No obstante, no es la única forma en que le brinda soporte financiero. De hecho, un informe del Departamento del Tesoro de los EEUU¹¹⁹ indica que el apoyo iraní ha hecho posible las actividades terroristas de tal or-

¹¹⁵ COMISIÓN EUROPEA. “Desmitificando los Tokens No Fungibles o NFT”. *Diario La Ley*, 2021, s/p. Recurso electrónico recuperado del siguiente enlace: <https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyTDA2MzZUK0stKs7Mz7M1AooYGhkagAQy0ypd8pNDKgtSbdMSc4pTAaJefJw1AAAWKE>. Consultado por última vez el día 10 de julio de 2025.

¹¹⁶ L. HINOJOSA. *La financiación del terrorismo y las Naciones Unidas*. Editorial Tecnos, 2008, pág. 73. El autor insiste en que la normativa internacional exige a los Estados que se abstengan de financiar grupos terroristas.

¹¹⁷ L. DE LA CORTE IBÁÑEZ. *La lógica del terrorismo*. Alianza Editorial, 2006, pág. 139.

¹¹⁸ Hace referencia a quienes tienen poder político, económico o social -aunque especialmente político- valiéndose del cual cometan delitos impunemente. En cuanto a lo primero, al tener influencia en la propia construcción de las leyes y el poder ejecutivo del Estado, se aprovechan de esa posición para eludir los mecanismos de control penal. *Vid. J. ÁLVAREZ LEÓN & F. GARCÍA ASTUDILLO. “La no renovación de la clase gobernante y la cifra dorada. Una visión criminológica de la impunidad en México”*. *Revista del Posgrado en Derecho de la UNAM*, núm. 19, 2022, pág. 99.

¹¹⁹ DEPARTAMENTO DEL TESORO DE LOS ESTADOS UNIDOS. “United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers” [Comunicado de Prensa], 14 de noviembre de 2023, s/p. Recurso electrónico recuperado del

ganización, que incluye “la transferencia de cientos de millones de dólares en asistencia financiera y el suministro de armas y entrenamiento operativo”. Esto ha hecho que Estados Unidos y Reino Unido impongan sanciones a Irán por contravenir el Derecho Internacional. Y es que Hamás se enfrenta a sanciones y se encuentra fuera del sistema bancario internacional. Por eso no es de extrañar que sus fuentes de apoyo opten por las criptomonedas, como un vehículo económico traspuesto con respecto a las estructuras financieras ordinarias. Por ejemplo, Qatar y Turquía, argumentando que los fondos que ofrecen es para los palestinos y no para financiar las actividades propias de Hamás, han acabado respaldando sus actos y las criptomonedas han facilitado estos movimientos económicos¹²⁰.

3.3. Poseer

La posesión es definida por la RAE¹²¹ como “tener en su poder algo”. La trabañón de tantas conductas típicas en un mismo precepto equipara su nivel de injusto. De esta forma, el legislador entiende igual de grave a quien utiliza bienes con fines terroristas y a quien es un mero poseedor de los mismos. A juicio de NAVARRO CARDOSO¹²², esto confunde las nociones de participación y autoría y puede llegar a ser tan anfibológico como “el sujeto que lleva en el propio vehículo a un vecino que se lo encuentra en el zaguán, o en la parada de guaguas, sabiendo que porta dinero para financiar a la organización terrorista a la que él sabe que el vecino pertenece; o en el sujeto que facilita el contacto de un receptor de bienes sustraídos sabiendo que la ganancia obtenida va a estar destinada a financiar a la organización terrorista a la que pertenece el que recibe la información”. Afirma el autor mencionado que el sujeto activo de estos ejemplos sin duda realiza una actividad con los bienes, pero de forma muy indirecta como para asumirlo parangonable con el que realiza otras conductas del tipo. Ahora bien, es difícil imaginar un escenario en que un sujeto u organización posea fondos con finalidad terrorista, sin que esa posesión implique otras actividades ya castigadas en el tipo penal.

siguiente enlace: <https://home.treasury.gov/news/press-releases/jy1907>. Consultado por última vez el día 19 de marzo de 2025.

¹²⁰ K. PLADSON. “Cómo las criptomonedas facilitaron el ataque de Hamás” [Artículo de Prensa]. DW, 16 de octubre de 2023, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.dw.com/es/c%C3%B3mo-las-criptomonedas-facilitaron-el-ataque-terrorista-de-ham%C3%A1s-contra-israel/a-67114348>. Consultado por última vez el día 10 de julio de 2025.

¹²¹ REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española* (23^a Edición), 2014. Consultese en el siguiente enlace: <https://www.rae.es/drae2001/poseer>.

¹²² F. NAVARRO CARDOSO. “Los tipos dolosos del delito de financiación del terrorismo”. *Op. Cit.*, pág. 14.

En el entorno cripto, “poseer” no debe entenderse como la tenencia física de bienes¹²³, sino el acceso a una billetera virtual con poder de disposición sobre los fondos y/o el control de la comunidad de una criptomoneda específica. Así, se aprecian dos maneras en las que, con carácter general, se puede presentar la posesión cripto: a. la técnica, cuando se materializa con el control sobre las claves privadas de una *wallet* con disposición efectiva de los fondos que contiene y; b. la funcional, cuando lo que se posee es la capacidad de influir en la forma en que se utilizan fondos dentro de una comunidad cripto. Esto es importante puesto que la posesión de fondos con fines terroristas se externaliza de manera idéntica a la posesión legítima en el contexto de los activos virtuales. Y aunque también ocurre esto en muchos casos de la financiación terrorista, la posibilidad de investigación y control es distinta cuando se trata de fondos cripto. Estos últimos no se pueden asociar fácilmente la posesión un contexto físico y social reconocible, como una empresa, lugar o persona. Tal grado de opacidad hace que sea necesario emplear métodos avanzados de trazabilidad (análisis de transacciones, patrones de comportamiento...) para intentar inferir la intención de la posesión de fondos, a partir de las transacciones recibidas o emitidas. Al incorporar estos elementos, la conducta deja de tratarse de una mera posesión, incluyendo otros comportamientos incluidos en el tipo penal.

Los terroristas pueden mantener fondos criptográficos bajo su control con el objetivo de especular con ellos y producir ganancias pasivas. Ciertamente, asumir a las criptomonedas como objeto de inversión es riesgoso por su alto nivel especulativo. Debido a lo anterior, los terroristas optan preferentemente por *stablecoins*. Por ejemplo, el ISKP utiliza este tipo de criptomonedas para almacenar fondos que previamente obtiene a través de Monero¹²⁴. Asimismo, agencias de inteligencia israelíes han advertido que las monedas estables USDT, USDC y USDD en la red Tron son un conducto importante para canalizar fondos a Hamás, ISIS y Hezbollah¹²⁵. El uso de criptomonedas estables con fines terroristas es una de las máximas preocupaciones de los operadores jurídicos y finan-

¹²³ De hecho, en alguna ocasión se ha llegado a señalar que las criptomonedas no tienen posesión. Es el caso, por ejemplo, del documento publicado por TRADE REPUBLIC. Información sobre el riesgo de las operaciones con criptomonedas, 2024, pág. 4. Recurso electrónico recuperado del siguiente enlace: <https://assets.traderepublic.com/assets/files/Crypto%20ES%20Disclaimer%20Document.pdf>. Consultado por última vez el día 10 de julio de 2025. En el mismo, la empresa financiera señala que “las criptomonedas no tienen propiedad y tampoco posesión”, pues lo que se posee son las claves necesarias para acceder a los fondos. Por tanto, la posesión se resumiría a su juicio con la custodia de dichas claves. En el mismo sentido, G. MOORE. “Custody. Crypto Assets’ Unique Challenge and Opportunity”. Coindesk, 2019, pág. 4; afirma que tener criptomonedas significa “poseer una contraseña criptográfica o clave privada”, lo que permite acceder y controlar una parte concreta del registro global de esa criptomoneda.

¹²⁴ TRM. *Crypto Crime Report*, 2025, pág. 12.

¹²⁵ THE COINOMIST. “Terrorist groups are actively using stablecoins” [Artículo de prensa], 16 de octubre de 2023, s/p. Recurso electrónico recuperado del siguiente enlace:

cieros¹²⁶. Los factores que toman en cuenta los terroristas para elegir un medio de financiación son las siguientes, según DION-SCHWARZ, MANHEIM y JOHNSTON¹²⁷: anonimato, usabilidad, seguridad, amplia aceptación, fiabilidad y volumen. Las *stablecoins* cumplen todos esos factores, salvo la amplia aceptación y, en cierta medida la usabilidad¹²⁸. Para evitar que la estabilidad relativa de este tipo de activos virtuales pueda ser aprovechado para la comisión de delitos terroristas, se necesita un marco de respuesta eficaz que abarque medidas de gestión de riesgos, una gobernanza y supervisión global con cooperación transfronteriza y comunicación, consultas y apoyo efectivos y mutuos¹²⁹.

También es posible que los terroristas creen una criptomoneda propia y ostentar el control de la comunidad para guardar fondos; una forma clara de posesión en sentido estricto. Esto no se ha producido directamente en la práctica o, al menos, no se ha podido consultar ningún estudio que así lo compruebe, pero la posibilidad existe y no debe descartarse como escenario futuro o incluso presente. Tal como se explicó en el primer bloque de este trabajo, las criptomonedas funcionan a partir de protocolos colaborativos donde la validación y funcionamiento de la red dependen de la interacción entre nodos y participantes. En la mayoría de los casos, cuando la mayoría absoluta de los integrantes de la red alcanza consenso, pueden controlar la comunidad y las decisiones técnicas que les afectan. Esto es posible, eso sí, solo en el caso de redes privadas o bajo uso. Si se trata de una cadena de bloques grande, como Bitcoin o Ethereum, eso es prácticamente imposible. Ahora bien, si un grupo terrorista crea su propio *token* y lo lanza en una blockchain pública o privada¹³⁰, asegurándose de que sus miembros y colaboradores representan esa clara mayoría, podrían quemar unidades de ese *token*, detener

ce: <https://coinomist.com/breaking-news/terrorist-groups-are-actively-using-stablecoins/>. Consultado por última vez el día 10 de julio de 2025.

¹²⁶ BANCO CENTRAL EUROPEO. "Stablecoins – no coins, but are they stable?". *In Focus*, núm. 3, 2019, pág. 2. Los autores K. SOOD, S. SINGH, A. BEHL, R. SINDHWANI, S. KAUR & V. PEREIRA. "Identification and prioritization of the risks in the mass adoption of artificial intelligence-driven stable coins: The quest for optimal resource utilization". *Resources Policy*, vol. 81, 2023, pág. 12; sitúan los riesgos delictivos como la tercera mayor preocupación de los reguladores y responsables de políticas públicas.

¹²⁷ C. DION-SCHWARZ; D. MANHEIM & P. JOHNSTON. *Terrorist Use of Cryptocurrencies*. *Op. Cit.*, pág. 33. Los autores afirman que de los factores mencionados los más importantes son el anonimato, para evitar la atención y detección por parte de las autoridades, y la fiabilidad y el volumen, porque se usarán para transferir grandes cantidades de activos.

¹²⁸ K. SOOD, S. SINGH, A. BEHL, R. SINDHWANI, S. KAUR & V. PEREIRA. "Identification and prioritization of the risks in the mass adoption of artificial intelligence-driven stable coins: The quest for optimal resource utilization". *Op. Cit.*; indican que la mayoría de las emisoras de *stablecoins* mantienen sus activos de reserva internamente, generando una mayor desconfianza del público general hacia estos activos.

¹²⁹ C. LI & Y. SHEN. "The potential impacts and risks of global stablecoins". *China Economic Journal*, vol. 14, núm. 1, 2021, pág. 50.

¹³⁰ Las *blockchains* públicas consisten en una red abierta y de acceso público, con transacciones cuya lectura es visible para cualquier participante de la red. Por el contrario, las

temporalmente cualquier transferencia del mismo, impedir que determinados usuarios lo usen, etc. Si esto se produce, es aún más férrea la ausencia de una autoridad que prevenga y controle el abuso del sistema¹³¹, poniendo en peligro incluso la estructura descentralizada de la red. Se le ha consultado a ChatGPT cómo se puede crear un token terrorista para poseer fondos con fines criminales y, no solo ha indicado genéricamente cómo, sino que ha suministrado el código y la implementación en *Solidity*¹³² para lograrlo en poco tiempo y sin esfuerzos. La máquina de IA lo ha llamado TerrorCoin (TCO):

¡Perfecto! Te muestro cómo crear una criptomonedra básica (un token ERC-20) en la red Ethereum. Este tipo de token es estándar y fácil de implementar con Solidity (el lenguaje de Ethereum).

Ejemplo de Token ERC-20 Simple: TerrorCoin (TCO)

⚠️ Nota importante: Esto es solo con fines educativos y técnicos. No apoyamos ni promovemos actividades ilegales ni uso indebido de tecnología.

💡 ¿Qué hace este contrato?

- Crea un token llamado `TerrorCoin (TCO)`.
- Tiene una cantidad inicial definida (ej. 1 millón de tokens).
- Permite transferencias y aprobaciones entre usuarios.
- Compatible con billeteras y exchanges que aceptan el estándar ERC-20.

💡 ¿Cómo se implementa?

1. Ambiente de desarrollo:
 - Usa Remix IDE (web).
 - Selecciona compilador Solidity 0.8.x.
2. Red de prueba (testnet):
 - Conecta Metamask a Goerli o Sepolia.
 - Obtén ETH de prueba desde un faucet.
 - Despliega el contrato.
3. Coste en red real (Mainnet):
 - Desplegar en Ethereum cuesta varios cientos de dólares en gas.
 - Alternativas más baratas: Binance Smart Chain, Polygon, Fantom.

Gráfica 1: Respuesta de ChatGPT sobre la creación de una criptomonedra propia por parte de grupos terroristas.

Fuente: *OpenAI. Prompt* propio

El código informático base suministrado por la máquina¹³³ y el que corresponde a funcionalidades específicas del *token*, fueron enviados a

privadas son aquellas a las que solo se puede acceder con invitación previa y la lectura de sus transacciones es posible si se obtienen permisos.

¹³¹ R. ANGGRIAWAN & M. ENDRIYO. "Cryptocurrency and Its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations". *Op. Cit.*, pág. 263.

¹³² Es un lenguaje de programación orientado a la escritura e implementación de contratos inteligentes en varias plataformas blockchain. Se ha estudiado en diversas investigaciones, con el fin de establecer un medio técnico que permita analizar y predecir comportamientos ilícitos y/o vulnerabilidades. Por ejemplo, *vid.* E. ABDULLAIEVA & L. GALCHYNSKY. "An Algorithm for Analyzing the Ethereum Network Blockchain to Detect Illegal Activities". *Theoretical and Applied Cyber Security*, vol. 6, núm. 1, 2024, págs. 43, 46 y ss, que proponen un modelo de minería de datos y; S. SCHMEELK; B. ROSADO & P. BLACK. "Blockchain Smart Contracts Static Analysis for Software Assurance". *Intelligent Computing Proceedings of the 2021 Computing Conference, Volume 2*, Springer, vol. 284, 2021, pág. 887, quienes recomiendan el desarrollo de herramientas de análisis estático de *Solidity* en sus diversas versiones, entre otras cosas, para atender a riesgos legales.

¹³³ En realidad, el ERC-20 es un estándar destacado de Ethereum para tokens y su interoperabilidad. Dada su amplia utilización y uso generalizado, no son pocas las vulnerabilidades que tiene. *Vid.* R. RAHIMIAN & J. CLARK. "TokenHook: Secure ERC-20 smart contract". *arXiv*, núm. 2107.02997, 2021, pág. 1. Pero son código disponible en abierto. De hecho, al preparar este apartado se han podido consultar varios Trabajos de Fin de Grado y Trabajos de Fin de Máster desarrollando *smart contracts* con este modelo o patrón.

un desarrollador de *software* con dilatada experiencia en el área¹³⁴, quien ha indicado lo siguiente: “El código producido es relativamente simple, no sólo por estar organizado en funciones sencillas y de responsabilidad única, sino porque estructura las operaciones que se pueden realizar sobre la criptomoneda propuesta de forma intuitiva y básica. Esto hace que el código sea muy legible para cualquier persona, aun cuando tenga un nivel básico de conocimientos en programación. De hecho, las operaciones definidas, incluso las “avanzadas”, se especifican de forma muy general, ya que son conceptos que podrían aplicar a numerosas estructuras de datos, no necesariamente relacionadas con el mundo de las criptomonedas, tales como listas, conjuntos, colas, entre otras. Entre estas operaciones están las transferencias, especificadas como un simple incremento/ decremento en el valor (o saldo) de un elemento de la lista, o las listas negras, estructuradas como una lista adicional de ‘entidades’ (o cuentas) sobre los cuales no se pueden realizar operaciones”. Si a lo expuesto por el profesional se le suma que es posible acceder al código en segundos con la ayuda de la IA, no cabe duda de que se trata de un problema serio con implicaciones profundas en materia de seguridad.

Los terroristas también pueden poseer fondos en monederos fríos, asumiendo ellos su custodia al apuntar o guardar las claves en un papel o dispositivo físico¹³⁵. Es una opción mucho más segura que las *hot wallet*, debido a que no dependen de conexiones a Internet y son menos vulnerables a ataques digitales. Más aún porque, en muchos casos los terroristas se conectan a redes *wifi* públicas¹³⁶, lo que puede comprometer la seguridad de los monederos conectados y aumentar el riesgo de interceptación. Por otra parte, las *cold wallets* tienen el peligro de perdida definitiva si de extravía el soporte donde se resguardan y, por eso, deberían estar sujetas a mecanismos de auditoría continua y rotaciones¹³⁷ que garanticen tanto su integridad como la disponibilidad de los fondos en caso de incidentes

¹³⁴ Consulta a Abel Josué Francisco Agra, Ingeniero Informático egresado de la Universidad Simón Bolívar y Máster en Ingeniería Informática por la Universidad de Granada, con más de 15 años de experiencia en el desarrollo y consultoría informática, realizada el día 16 de abril de 2024. Se le expuso la respuesta del *ChatGPT* y se le inquirió su opinión técnica al respecto, la cual fue remitida directamente por correo a la autora de este trabajo.

¹³⁵ A. DÍAZ BERNARDOS. “Explorando las huellas digitales de los criptoactivos mediante fuentes abiertas”. *Ciencia Policial*, núm. 182, 2024, pág. 280; distingue los monederos fríos de los mixtos, al señalar que los primeros registran las claves en papel y los segundos en un dispositivo físico. Se advierte que esta no es una categorización aceptada a nivel general, se destaca para que el lector conozca diversas opiniones.

¹³⁶ F. JOHANNES TEICHMANN. “Financing terrorism through cryptocurrencies – a danger for Europe?”. *Journal of Money Laundering Control*, vol. 21, núm. 4, 2018, págs. 515 y 516.

¹³⁷ P. CHATZIGIANNIS & K. CHALKIAS. “Proof of Assets in the Diem Blockchain”. *Applied Cryptography and Network Security Workshops*. ACNS 2021 Satellite Workshops AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA Kamakura, Japan, June 21–24, 2021, Proceedings. Jianying Zhou et.al (eds.). Springer, 2021, pág. 35.

o accesos no autorizado. Esto es un trabajo extra para los terroristas que podrían no querer aceptar.

Por otra parte, la posesión de fondos puede no ser perpetrada por terroristas activos directamente. En primer lugar, esto puede llevarse a cabo por las llamadas “células durmientes”, definidas por un documento de la Asamblea General y del Consejo de Seguridad de las Naciones Unidas¹³⁸ como redes dispersas por todo el mundo que se abocan a llevar a cabo actividades terroristas autónomas —como el caso de los lobos solitarios— y que “pueden estar formadas por individuos no afiliados a entidades terroristas, pero que comparten la misma ideología islamista radical”. Además, advierte que estas utilizan activamente la tecnología moderna para llevar a cabo diversas fases y formas de la actividad terroristas. Por eso, siguen estando vigentes las palabras de ARISTEGUI¹³⁹: “debemos saber que luchar contra estas células, ya sean activas o durmientes, es una tarea cada vez más compleja que exige especialistas cada vez más cualificados”. La posesión de bienes o fondos para financiar actividades terroristas puede ser aún más difícil de rastrear si esta corresponde a individuos o agrupaciones de ellos que no están activamente relacionados con organizaciones criminales de este tipo.

En relación con la ofuscación de los verdaderos poseedores de fondos, los terroristas pueden optar por servicios de custodia de criptomonedas clandestinos o al margen de la regulación. Los avances regulatorios han tendido a incluir a los servicios de custodia dentro de los sujetos obligados por la normativa de lucha contra la financiación del terrorismo y, en virtud de ello, son operadores sometidos a estrictos controles, que incluyen la diligencia debida, la verificación de identidad de usuarios y el reporte de transacciones sospechosas. Además, como tal, quienes prestan servicios de custodia están sujetos y no exentos del Impuesto sobre el Valor Añadido de conformidad con lo expresado en la Consulta Tributaria N° V2679-21 de la Subdirección General de Impuestos sobre el Consumo. En cuanto a las obligaciones fiscales, los titulares reales de las criptomonedas o quienes ostentan poder de disposición sobre ellas están obligados a cumplimentar y presentar debidamente el modelo 721 de la Agencia Tributaria española, identificando con claridad cada tipo de moneda virtual, la empresa o persona física que proporciona servicios para salvaguardar las claves criptográficas privadas en nombre de terceros o mantener (poseer) monedas virtuales, entre otras cuestiones. En caso de

¹³⁸ NACIONES UNIDAS. Carta de fecha 11 de marzo de 2020 dirigida al Secretario General por el Representante Permanente de la Federación de Rusia ante las Naciones Unidas. Documento con referencia A/74/751-S/2020/204, preparado por la Reunión de Jefes de Servicios Especiales, Organismos de Seguridad y Órganos Encargados del Cumplimiento de la Ley, asumido como documento de la Asamblea General y del Consejo de Seguridad de las Naciones Unidas, 2020, págs. 2 y 7.

¹³⁹ G. ARISTEGUI. “El nuevo terrorismo”. En *Cuenta y razón del pensamiento actual*, núm. 126, 2002, pág. 30.

que los terroristas quieran delegar este servicio, optarían por *exchanges off shore* sitos en jurisdicciones con poca supervisión financiera o de intervención punitiva baja en materia de anti financiación del terrorismo. También pueden valerse de las billeteras de criptomonedas de la Web 3.0, como *Metamask* o *Trust Wallet*, que no son propiamente servicios de custodia de criptomonedas pero sí billeteras donde almacenar criptomonedas. Algunas, como la primera de las mencionadas, son *wallets* que funcionan como la extensión de un navegador de Internet que actualmente tienen muchos usuarios. Sin embargo, tampoco son modelos eficientes puesto que hay investigaciones que reconocen la posibilidad de analizar a nivel forense y extraer pruebas digitales del uso ilícito de estas herramientas¹⁴⁰.

3.4. Utilizar

Entendiendo este verbo de la forma en que lo hace la RAE¹⁴¹, es decir, “hacer que algo sirva para un fin”, es evidente que los terroristas se valen de los fondos que reciben y poseen para sostener sus campañas violentas¹⁴². Estos delincuentes utilizan sus medios económicos para una variedad de objetivos concretos: adquirir armas, captar y adiestrar nuevos miembros, perpetrar atentados¹⁴³... En resumen, necesitan fondos para financiar actividades logísticas de tipo organizacional y operativo y tácticas, manteniendo una infraestructura económico-financiera proyectada al cumplimiento de sus metas criminales¹⁴⁴. En realidad, todas las conductas anteriores de financiación del terrorismo existen para llegar, al menos, a utilizar esos bienes o tener la intención de hacerlo. Por eso, las

¹⁴⁰ Por ejemplo, J. KIM, et. al. “A Study on the Digital Forensics Artifacts Collection and Analysis of Browser Extension-Based Crypto Wallet”. *Journal of the Korea Institute of Information Security & Cryptology*, vol. 33, núm. 3, 2023, págs. 476 y 477; exponen que el análisis del IP y el caché y las *cookies* concretamente puede ser útil para obtener datos forenses de billeteras criptográficas basadas en extensiones del navegador. Por su parte, M. MERAJ, A. OZER & U. KARABIYIK. “Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS”. *Applied Sciences*, vol. 12, núm. 21, 2022, pág. 32; proponen la técnica de reconstrucción automática de eventos, entre otros métodos, recuperando los sitios y servicios consultados en línea por los usuarios.

¹⁴¹ REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española* (23^a Edición), 2014. Consultese en el siguiente enlace: <https://dle.rae.es/utilizar>.

¹⁴² M. BUESA BLANCO. “Financiación del terrorismo”. *Op. Cit.*, pág. 46.

¹⁴³ NACIONES UNIDAS. Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo. Informe del Secretario General, 2006, pág. 9.

¹⁴⁴ ORGANIZACIÓN DE ESTADOS AMERICANOS. *Guía Práctica de Prevención, Deteción y Represión del Financiamiento del Terrorismo*, 2007, págs. 108 y 109. Al respecto, afirma el Comité Interamericano Contra el Terrorismo que estas acciones son propias del terrorismo internacional, puesto que no necesariamente el país destinatario de esos fondos o donde se ejecuta el atentado es el mismo que donde se obtuvieron aquellos.

estrategias gubernamentales y de política criminal pretenden intervenir antes de alcanzar este culmen. Eso, como menciona MERINO HERRERA¹⁴⁵, constituye un “mecanismo para imprimir un fuerte golpe a la base económica de estas organizaciones criminales”.

La experiencia práctica ha demostrado que los terroristas han encontrado en las criptomonedas un instrumento eficaz para utilizar esos fondos, incluso sin necesidad de convertirlos en dinero fiduciario. En primer lugar, estos delincuentes pueden hacer compras de bienes y servicios ilícitos en la *Dark Web* que sean necesarios para potenciar o ejecutar sus actividades¹⁴⁶. En este mismo espacio también pueden utilizar los fondos para gestionar actividades preparatorias, como adquirir documentación falsa o robada y armamento¹⁴⁷. Por eso, existen múltiples recursos que los servicios y unidades de inteligencia han desarrollado y perfeccionado para combatir las acciones delictivas en la dark web, especialmente las relacionadas con el terrorismo. Entre las iniciativas destacadas se encuentra el proyecto DANTE¹⁴⁸ financiado por la Comisión Europea, el cual ejemplifica el uso de la Inteligencia Artificial como herramienta de apoyo en la lucha contra el crimen. Este proyecto emplea, entre otras tecnologías, sistemas desarrollados por *Expert System*, los cuales permiten, mediante análisis contextual de textos, identificar lenguaje yihadista, localizar personas adoctrinadas, detectar información falsa y reconocer patrones comunes en redes sociales.

Un caso reciente es el de un grupo europeo de extrema derecha autodenominado *Order of Down*. Su objetivo es crear un ejercito de voluntarios para atacar embarcaciones de migrantes y sus colaboradores, por considerarlos como invasores, y una milicia independiente contra ISIS¹⁴⁹. En 2018 inició una campaña de financiación en línea, exhortando a los interesados a donar con Monero. El grupo indicaba que de esa forma el donante “se convertía en parte de la historia”, pues esos recursos irían destinados a tales ataques violentos. Entre otras cosas, exponían

¹⁴⁵ J. MERINO HERRERA. “Estrategias de persecución penal contra la financiación del terrorismo”. En *Revista Penal México*, núm. 8, 2015, págs. 118 y 124.

¹⁴⁶ J. TAMARIT SUMALLA. “Ciberterrorismo. Regulación y estrategias para combatirlo”. Universitat Oberta de Catalunya, 2020, pág. 12.

¹⁴⁷ D. MONTES NOBLEJAS. “A vueltas con el terrorismo e Internet: Hacia una definición de ciberterrorismo”. En *Revista de Derecho UNED*, núm. 27, 2021, pág. 727.

¹⁴⁸ La presentación oficial del proyecto DANTE se puede consultar en el siguiente enlace: <https://www.h2020-dante.eu/wp-content/uploads/2016/10/Dante-Brochure.pdf>. El documento expone que se trata de un sistema integrado basado en minería y análisis de datos para analizar una gran cantidad de contenidos heterogéneos y complejos relacionados con el terrorismo en la Internet profunda y la Internet oscura.

¹⁴⁹ COUNTER EXTREMISM PROJECT. “Far-Right European Terrorist Group Crowdfunding Cryptocurrency” [Nota de Prensa], agosto de 2018, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency>. Consultado por última vez el día 10 de julio de 2025.

que con tal criptomoneda privada comprarían armas de fuego y explosivos, equiparían al ejército, establecer una flota naval, refugios, redes continentales o centros de movilización¹⁵⁰. Por su parte, la facción yihadista Hay'at Tahrir al-Sham (HTS), antiguo afiliado de Al-Qaeda se ha valido de una empresa llamada *BitcoinTransfer* para hacer negocios con criptomonedas. De hecho, una investigación de WIRED¹⁵¹, define a la plataforma como una red que proporciona dinero a grupos terroristas y que fungió como “centro neurálgico en seis operaciones de financiación del terrorismo”. Un ejemplo similar se aprecia en un *bot* de *Telegram* pro Al-Qaeda que pedía donaciones con criptomonedas para dirigir esos fondos en células operativas de la organización, con el fin de cubrir las necesidades básicas de sus miembros, como alimentos, combustible y atención médica¹⁵².

Según DAVIS¹⁵³, los fondos terroristas también pueden utilizarse de forma ocasional o puntual para suministrar flujos de efectivo —o de criptomonedas— a subgrupos que dieron financiación inicial o para mantener una marca global. En este sentido, la propaganda terrorista es clave para la construcción y permanencia de dicha marca. El terrorismo contemporáneo se vale de canales de comunicación independientes y dinámicos; de innovaciones tecnológicas, como cámaras digitales o programas especiales de producción de recursos audiovisuales y; de plataformas multilingües en línea¹⁵⁴. Y esto supone gastos económicos. Un proyecto que informa semanalmente sobre los métodos que utilizan los extremistas para explotar Internet y conseguir más adeptos informó que un grupo pro ISIS promovía en un chat de *Telegram* el uso de Monero para financiar propaganda en línea¹⁵⁵. Las criptomonedas, por ende,

¹⁵⁰ S. WARRETH. “Crowdfunding and Cryptocurrency Use by Far-Right and Jihadi Groups” [Artículo de Prensa]. Vox Pol, 2019 (actualizado en 2024). Recurso electrónico recuperado del siguiente enlace: <https://voxpol.eu/crowdfunding-and-cryptocurrency-use-by-far-right-and-jihadi-groups/>. Consultado por última vez el día 10 de julio de 2025.

¹⁵¹ R. O'LEARY. “The bitcoin terrorists of Idlib are learning new tricks” [Artículo de Prensa]. WIRED, 2021, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.wired.com/story/bitcoin-crypto-terrorism-syria/>. Consultado por última vez el día 18 de abril de 2024.

¹⁵² MEMRI. “Pro-Al-Qaeda Telegram Bot Solicits Cryptocurrency Donations For ‘Operational Cell’ In Gaza” [Nota de Prensa], octubre de 2023, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.memri.org/cjlab/pro-al-qaeda-telegram-bot-solicits-cryptocurrency-donations-operational-cell-gaza>. Consultado por última vez el día 10 de julio de 2025.

¹⁵³ J. DAVIS. “The Financial Future of the Islamic State”. En *CTC Sentinel*, vol. 17, núm. 7, 2024, pág. 33.

¹⁵⁴ Así lo expone M. CANO PAÑOS. “Odio e incitación a la violencia en el contexto del terrorismo islamista. Internet como elemento ambiental”. *InDret Revista para el Análisis del Derecho*, núm. 4, 2016, pág. 5; aunque el autor contextualiza estos factores a la denominada “ciberyihad”.

¹⁵⁵ COUNTER EXTREMISM PROJECT. “Extremist Content Online: Pro-ISIS Online Chat Promotes Monero Cryptocurrency To Fund Propaganda Operations” [Nota de Prensa], junio de 2023, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www>

también están siendo utilizadas por grupos o individuos terroristas para financiar sus campañas de propaganda. Esto propicia un ciclo de retroalimentación negativa porque, a medida que la propaganda se expande, atrae más simpatizantes y potenciales donantes, lo que a su vez incrementa el flujo de fondos disponibles para continuar y amplificar el mensaje violento.

Otros casos particulares en los que se han utilizado criptomonedas para financiar actos terroristas es para cubrir el pago de sobornos a funcionarios públicos a cambio de favores especiales o hacer transferencias a familias de combatientes de bajos recursos, como lo ha hecho Hamás con los millones de dólares que ha obtenido con sus campañas de financiación¹⁵⁶. Este ejemplo y los anteriores demuestra que la utilización de criptomonedas por parte de grupos terroristas es diversa y en constante evolución. Siendo así, es de suma importancia que las autoridades se mantengan actualizadas sobre las técnicas empleadas, con el fin de diseñar mecanismos eficaces de detección y programas de intervención temprana que permitan bloquear o rastrear los fondos vinculados al terrorismo antes de que sean empleados con fines delictivos altamente dañinos y de difícil contención posterior.

3.5. Convertir

La STS 279/2013 define a la conversión como la “transformación de bienes en otros distintos”. Este comportamiento es, en realidad, una expresión común en la actividad delictiva en la que intervienen fondos económicos. De hecho, es la fase final del llamado “triángulo del fraude”: se comete el acto ilegal, se oculta y se convierte el beneficio ilícito en alguna forma de beneficio útil¹⁵⁷. Esto es trasladable a los terroristas, quienes necesitan transformar sus activos en bienes, herramientas o elementos útiles para el desarrollo de sus actividades. La conversión de fondos cripto es uno de las grandes ventajas de usar este entorno digital para la financiación del terrorismo. En poco tiempo y con comisiones mínimas, pueden transformar dichos activos, bien para ocultar su origen, bien para

counterextremism.com/press/extremist-content-online-pro-isis-online-chat-promotes-monero-cryptocurrency-fund-propaganda. Consultado por última vez el día 10 de julio de 2025.

¹⁵⁶ G. PACCHIANI. “Terrorists raised \$130m in crypto since 2021; sought more via social media after attack” [Artículo de Prensa]. The times of Israel, octubre de 2023, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.timesofisrael.com/gaza-terror-groups-raised-over-130-million-in-crypto-to-fund-attack/>. Consultado por última vez el día 10 de julio de 2025.

¹⁵⁷ S. WANG & X. ZHU. “Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing”. *Policing: A Journal of Policy and Practice*, vol. 15, núm. 4, 2021, págs. 2330 y 2331.

movilizarlo posteriormente o bien para adquirir otros fondos. Los terroristas pueden convertir sus activos digitales en dinero *fiat* o viceversa, en otros criptoactivos (criptomonedas de privacidad, preferiblemente)¹⁵⁸ o para comprar bienes y servicios, frecuentemente en la *Dark Web*¹⁵⁹.

La conversión de bienes criptográficos con fines terroristas puede lograrse a través de técnicas ya consideradas en este trabajo. Por ejemplo, mediante servicios de intercambio de criptomonedas¹⁶⁰, criptocajeros, plataformas de juego con criptomonedas¹⁶¹, uso de *bridges* y *mixers*¹⁶², la tokenización de activos y otros. Estos mecanismos favorecen la transformación de fondos con un mayor nivel de privacidad o anonimato, disociando la fuente original de los mismos. En todos los casos mencionados, se altera la forma o naturaleza del bien en cuestión, para asegurar su disponibilidad y utilidad para la comisión de actos terroristas o el sostenimiento de sus estructuras y redes organizativas. Además, la conversión de bienes terroristas en entornos criptográficos implica la coexistencia de comportamientos materiales y digitales, por lo que las labores de rastreo e investigación deben orientarse hacia ambas perspectivas. No obstante, la estricta conversión de fondos puede ser muy complicada de detectar, cuando no hay movimientos sospechosos previos o posteriores.

Por tanto, según el tipo de bien de origen y destino, la conversión de fondos cripto con fines terroristas puede ser: de cripto a *fiat*, de *fiat* a cripto, de cripto a cripto, de cripto a otros activos físicos o digitales y viceversa. Pero también se pueden clasificar estos movimientos según la finalidad funcional de la operación (si es para ocultar el origen de los fondos, para movilizarlos, para diversificar el riesgo...), o según el canal tecnológico utilizado. Sin embargo, la última opción es metodológicamente limitada y poco práctica, pues quedaría desfasada cada vez que una no-

¹⁵⁸ S. ALI IBRAHIM. "Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing". *Pakistan Horizon*, vol. 74, núm. 1, 2021, pág. 77.

¹⁵⁹ En el estudio de P. CARROLL & J. WINDLE. "Cyber as an enabler of terrorism financing, now and in the future". *Journal of Policing, Intelligence and Counter Terrorism*, núm. 13-3, 2018, págs. 8 y 18; se considera un debate doctrinal sobre la explotación de los terroristas de nuevas tecnologías como las criptomonedas y la Internet oscura. Los autores analizan esta cuestión y concluyen que, si bien en algunos casos los terroristas prefieren el efectivo para muchos gastos, los criptoactivos brindan alcance internacional, facilidades y técnicas avanzadas para hacerlo.

¹⁶⁰ S. FARBER & S. YEHEZKEL. "Financial Extremism: The Dark Side of Crowdfunding and Terrorism". *Terrorism and Political Violence*, 2024, s/p. Versión electrónica recuperada del siguiente enlace: <https://www.tandfonline.com/doi/full/10.1080/09546553.2024.2362665>. Consultado por última vez el día 10 de julio de 2025.

¹⁶¹ A. MOVCHAN, et.al. "Investigating cryptocurrency financing crimes terrorism and armed aggression". *Social & Legal Studios*, vol. 6, núm. 4, 2023, pág. 127.

¹⁶² A. BURGESS, R. HAMILTON & C. LEUPRECHT. "Terror on the Blockchain: The emergent crypto-crime-terror nexus". *Financial Crime, Law and Governance. Navigating Challenges in Different Contexts*. Ius Gentium: Comparative Perspectives on Law and Justice, vol. 116, Doron Goldbarsht y Louis de Koker (eds.). Springer, 2024, pág. 209.

vedad en el entorno cripto facilite la transformación de fondos ya que el entorno cripto evoluciona de forma acelerada y tiende a hacer obsoletas las categorías puramente técnicas, sin que ello implique un cambio real en la lógica jurídica o delictiva de la conversión. Mas interesante en términos jurídicos resulta una taxonomía de conversión basada en la intervención humana, distinguiendo entre: a) conversiones manuales, donde el agente humano realiza la operación de forma consciente y secuencial, existiendo una mayor imputabilidad de responsabilidad sobre aquel; b) conversiones asistidas, basadas en el uso de herramientas informáticas —como *bots*, por citar un ejemplo—, donde el usuario ejecuta parte de la acción pero delega otra parte y; c) conversiones automatizadas, con un alto grado de automatización, dificultando la imputación de responsabilidad penal cuando han mediado procesos autónomos sobre los que el agente humano ha tenido poco o ningún control.

3.6. *Transmitir*

Finalmente, la STS 279/2013 entiende la transmisión como “extraer bienes de su patrimonio para integrarlo en el de un tercero”. En general, esta fase del financiamiento terrorista hace referencia a la transferencia de los fondos en cualquier forma de instrumento negociable o el traslado de los mismos a otras cuentas de sujetos delictivos o colaboradores en la misma o distinta jurisdicción¹⁶³. Tradicionalmente, las transferencias de fondos terroristas se distinguen en formales, como transferencias bancarias o envíos a través de entidades de pago formalizadas; e informales, más conocidas como método *hawala*¹⁶⁴.

3.6.1. La actualización del sistema “*hawala*” para transmitir fondos terroristas

El *hawala* es un sistema informal de transferencia de fondos, muy conocido como vía de financiación terrorista. De acuerdo con el Senado español tiene las siguientes características: se basa en la confianza entre

¹⁶³ De esa manera lo define M. DÓMINE. “Criminalidad económica y terrorismo”. *Revista de Derecho: Publicación de la Facultad de Derecho de la Universidad Católica de Uruguay*, núm. 1, 2006, pág. 124; destacando que dicha transferencia suele orientarse a realizar pagos de mercancías o servicios o suministrar fondos a la organización a la que se afilie ideológicamente. Las vías digitales de transmisión potencian y multiplican el efecto y alcance de tales movimientos. Es decir, se trata de un efecto multiplicador del delito. *Vid.* G. GADEA ALDAVE. “La política criminal de la Unión Europea con relación al terrorismo yihadista en internet” [Tesis de doctorado no publicada]. Universidad de Granada, 2024, págs. 49 y 50. Disponible en el repositorio abierto de la Institución: <https://digibug.ugr.es/handle/10481/81413>.

¹⁶⁴ M. MARTÍNEZ MARTÍNEZ. “Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago”. *Revista de Pensamiento Estratégico y Seguridad CISDE*, núm. 1, 2016, pág. 71.

usuarios e intermediadores¹⁶⁵, es sencillo, rápido y anónimo, no se ve limitado por complicados procesos burocráticos —propio de su carácter informal¹⁶⁶— y resulta atractivo para distintos comportamientos del mercado ilícito por permitir movilizar grandes cantidades de dinero desde distintos lugares del mundo¹⁶⁷. A estas, el propio TS¹⁶⁸ añade las siguientes: menores costos de operación y comisiones más bajas, más seguridad y suponen una financiación extraoficial. El sistema comentado no es ilegal en sí mismo¹⁶⁹ —independientemente de los ilícitos que supone la evasión de impuestos y tasas que correspondan—, pero es susceptible de ser explotado por delincuentes y/o redes de crimen organizado. Especialmente se utiliza para blanquear fondos y para financiar actividades terroristas y constituye un reto para los servicios de inteligencia y los cuerpos de seguridad en lo que respecta a la determinación de sus fines ilícitos¹⁷⁰.

El funcionamiento del sistema *hawala* se fundamenta en redes personales entre distintos agentes. EL-QORCHI¹⁷¹ lo desarrolla muy bien: A quiere enviar dinero a B, pero como viven en zonas distintas necesitan intermediarios. Estos sujetos se conocen como *hawaladars*. A le da los fondos a uno de ellos (HA) y este a otro corresponsal de la región de B (HB), quien a su vez se encarga de que aquellos lleguen a su destinatario final. Los *hawaladars* reciben una remuneración a cambio de su trabajo. La organización de estos movimientos puede hacerse a través de locutorios telefónicos, carnicerías, tiendas de alimentación y bazares¹⁷², pero la interconexión es mucho más sencilla hoy en día gracias al Internet y las nuevas tecnologías. El modelo alternativo de envío de remesas que se

¹⁶⁵ Una de las diferencias entre el *hawala* y otros sistemas de transferencias informales de fondos es que el primero depende de sólidas creencias religiosas y culturales. *Vid. M. RAZAVY. "Hawala: An underground haven for terrorists or social phenomenon?". Crime, Law & Social Change*, núm. 44, 2005, pág. 279.

¹⁶⁶ Para algunos autores este es el aspecto distintivo más notorio del *hawala* con respecto a las transferencias financieras ordinarias. Un ejemplo de tal postura se halla en M. DE GOEDE. "Hawala discourses and the war on terrorist finance". *Environment and Planning D: Society and Space*, vol. 21, 2003, págs. 513 y 514. Este autor destaca que el sistema *hawala* escapa de los procedimientos contables formales y los registros oficiales, mientras que las transferencias de dinero realizadas por bancos internacionales se registran formalmente en balanzas de pago.

¹⁶⁷ SENADO ESPAÑOL. Respuesta del Gobierno a las preguntas 684/62456 y 684/62534, 684/64319 y 684/64414 y 684/64424. Secretaría de Estado de Relaciones con las Cortes y Asuntos Constitucionales, 2023, pág. 1.

¹⁶⁸ ATS 20770/2024, FJ 2.

¹⁶⁹ El *hawala* se utiliza para hacer transacciones financieras personales y comerciales, enviar remesas a familiares de migrantes y refugiados y otros. Al respecto, *vid. UNODC. "The Hawala System. Its operations and misuse by opiate traffickers and migrant smugglers". Afghan Opiate Trade Project y UNODC Research*, 2023, pág. 10.

¹⁷⁰ M. RANSTORP. "La financiación del terrorismo: principales actores, estrategias y fuentes". *Afskar*, Tendencias Económicas, 2018, pág. 55.

¹⁷¹ M. EL-QORCHI. "Hawala". *Finanzas y Desarrollo*, diciembre de 2022, pág. 32.

¹⁷² G. SÁNCHEZ MEDERO. "Las fuentes de financiación legales e ilegales de los grupos terroristas". *Op. Cit.*, pág. 64.

aborda en este epígrafe puede ser doméstico, cuando las transacciones se realizan en diferentes ciudades de un mismo país y; transfronterizo, cuando implica movimientos internacionales¹⁷³. Las organizaciones terroristas se estructuran en capas y redes verticales, horizontales y amorfas, según el caso. Debido a ello, el sistema clandestino de canalización financiera que es el *hawala* resulta muy útil para la transmisión de fondos entre sus células y miembros. Al Qaeda, por ejemplo, ha utilizado ampliamente tal modelo para movilizar dinero y bienes y financiar ataques determinados, obstaculizando la identificación del origen y destino de los mismos e impidiendo así que las agencias de inteligencia congelen sus activos¹⁷⁴. Esto ilustra, como afirma NÚÑEZ CASTAÑO¹⁷⁵, lo innumerables que son las vías por las que se pueden obtener los fondos necesarios para la realización de actividades terroristas y la vinculación cada vez más estrecha entre la criminalidad organizada y la terrorista.

Atendiendo a los riesgos del sistema *hawala*, el GAFI ha emitido la Recomendación Especial VI, sobre remesas alternativas¹⁷⁶: “Cada país debe tomar medidas para garantizar que las personas o entidades jurídicas, incluidos los agentes, que prestan servicios de transferencia de dinero o valor —incluida la transferencia a través de un sistema o red informal de transferencia de dinero o valor— estén autorizadas o registradas y sujetas a todas las Recomendaciones del GAFI que se aplican a los bancos e instituciones financieras no bancarias. Cada país debe asegurar que las personas o entidades jurídicas que realicen este servicio de manera ilegal estén sujetas a sanciones administrativas, civiles o penales”. El mismo Organismo internacional¹⁷⁷ señala, no obstante, que ha sido complicado en muchos países acercar al sector no regulado a medidas de cumplimiento, registro y supervisión¹⁷⁸. Así, el *hawala* sigue explotando

¹⁷³ N. JAWMAL. “Hawala-The Invisible Financing System of Terrorism”. *Strategic Analysis*, vol. 26, núm 2, 2022, s/p. Versión electrónica recuperada del siguiente enlace: https://ciaotest.cc.columbia.edu/olj/sa/sa_apr02jan01.html. Consultado por última vez el día 10 de julio de 2025.

¹⁷⁴ D. FAITH. “The Hawala System”. *Global Security Studies*, vol. 2, núm. 1, 2011, pág. 26.

¹⁷⁵ E. NÚÑEZ CASTAÑO. “El terrorismo en la era de la globalización: el delito de financiación del terrorismo ante el nuevo concepto de terrorismo”. *Globalización y lucha contra las nuevas formas de criminalidad transnacional*, Alfonso Galán y Silvia Mendoza (coords.). Editorial Tirant Lo Blanch, 2019. Consultada la versión electrónica en la Biblioteca online de Tirant.

¹⁷⁶ GAFI. IX Special Recommendations. Revisión de 2012. Recurso electrónico recuperado del siguiente enlace: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf>. Consultado por última vez el día 10 de julio de 2025.

¹⁷⁷ GAFI. “The role of hawala and other similar service providers in money laundering and terrorist financing”. Reporte, 2013, pág. 41.

¹⁷⁸ Cfr. J. DEL CID GÓMEZ. “A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates”. En *Perspectives on Terrorism*, vol. 4, núm. 4, 2010, pág. 15. En su estudio reconoce algunas jurisdicciones, como Emiratos Árabes Unidos y Afganistán, que han establecido normativas específicas para identificar a los remitentes y beneficiarios de los movimientos con el registro y supervisión de los *hawaladars*. Incluso, cuando estos ope-

vulnerabilidades para la financiación del terrorismo¹⁷⁹. España no obvia este riesgo y en la Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave, se establece la necesidad de mejorar los mecanismos de investigación de los pagos vinculados al terrorismo que se ejecutan al margen del sistema financiero, “en especial las redes tipo *hawala* y las transacciones con monedas virtuales”.

La llegada de las criptomonedas no ha sustituido el sistema *hawala*, sino que ha ofrecido opciones para potenciarlo y reconfigurarlo. Con tales activos los terroristas pueden prescindir del servicio de intermediarios y operar por ellos mismos, pero también pueden preferir mantener la presencia de aquellos para minimizar aún más el riesgo de detección, complicar la trazabilidad de los fondos, desbordar los sistemas regulatorios clásicos y diluir la responsabilidad en operaciones automáticas y/o fragmentadas. MIRABILE¹⁸⁰ considera que los sistemas de transferencias de activos basados en *blockchain* tienen características comunes con el sistema *hawala* tradicional¹⁸¹: canales alternativos para el envío de fondos y pagos, descentralización, actuación sin supervisión de una autoridad central, alcance local e internacional, entre otros. En la misma línea, VALERI et.al¹⁸² aprecian en la tecnología de cadena de bloques los mismos principios que inspiran el esquema *hawala*; a saber, la confianza, la comunidad, la privacidad y la descentralización.

radores son personas jurídicas, deben obtener una licencia y reportar las transacciones a unidades especializadas de inteligencia financiera.

¹⁷⁹ C. MALLADA. “La financiación del terrorismo desde la perspectiva de las nuevas tecnologías. A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo”. En *Anuario de Derecho Penal y Ciencias Penales*, vol. 71, 2018, pág. 250; destaca que la ausencia de normativas en el método *hawala* implica una ausencia de medios preventivos de hechos ilícitos como el KYC y la diligencia debida.

¹⁸⁰ M. MIRABILE. “Debating Hawala, Infrastructures and Critical Issues: A Continuum from Hawala to Blockchain Technologies?”. En *CONFines*, año 18, núm. 34, 2022, pág. 84.

¹⁸¹ En marzo de 2025 el Tribunal Supremo de India resolvió relacionado con *Bitcoin* y concluyó textualmente que “comerciar con *Bitcoin* en India es como tratar con un estilo refinado de comercio Hawala”. THE HINDU. “Trading in *Bitcoin* in India is refined way of doing Hawala business: Supreme Court” [Nota de prensa]. PTI, 6 de mayo de 2025. Recurso electrónico recuperado del siguiente enlace: <https://www.thehindu.com/news/national/trading-in-bitcoin-in-india-is-refined-way-of-doing-hawala-business-supreme-court/article69543528.ece>. Consultado por última vez el día 10 de julio de 2025.

¹⁸² M. VALERI, et.al. “The Use of Cryptocurrencies for Hawala in the Islamic Finance”. *European Journal of Islamic Finance*, núm. esp. EJIF Workshop, 2020, pág. 6. Los autores señalan que el uso de una *stablecoin* reduciría el riesgo de especulación para asegurar la rentabilidad de la operación. Además, proponen el lanzamiento de una “*globalcoin*” basadas en criptomonedas estables, que pueda ser adoptada por personas de todo el mundo mediante aplicaciones móviles comunes e intuitivas.

Ambos sistemas —el *hawala* tradicional y las criptomonedas— permiten transferencias de valor rápidas, sin limitaciones territoriales y al margen del alcance directo de los reguladores y supervisores estatales. Por eso son atractivos tanto para fines lícitos como ilícitos. En cuanto a los segundos, no son esquemas excluyentes entre sí. En el trabajo académico de MICCOLI¹⁸³ se expresa una forma en que ambos pueden combinarse: el proceso inicia con la compra de criptomonedas para mantener el anonimato, que luego se envían a un destinatario confiable. Este puede convertirlas en moneda local a través de un *hawaladar*, quien, en coordinación con otro *hawaladar* en el país emisor, se encarga del pago sin dejar rastros bancarios. Ambos intermediarios pueden saldar sus deudas usando criptomonedas, lo que dificulta aún más el seguimiento por parte de las autoridades. De acuerdo con esta idea, atender a las necesidades o vacíos regulatorios que el *hawala* supone en cada región es una forma indirecta de prevenir el uso de otras formas de transferencia informal, como las criptomonedas. También es posible que los *hawaladars*, en algún momento del proceso, requieran y utilicen servicios bancarios tradicionales y visibles en su jurisdicción. En su estudio, MARZHAN et.al¹⁸⁴ proponen el uso de redes neuronales gráficas aplicadas al ámbito financiero, para detectar fraudes y anomalías, especialmente estableciendo vínculos ocultos en cuentas bancarias o criptográficas. Sin embargo, no es una solución infalible pues en muchos casos los fondos nunca pasan por un canal bancario¹⁸⁵.

No obstante lo expuesto, también hay diferencias notorias entre el *hawala* y el uso de criptoactivos. La principal de ellas es que el primero se basa en la confianza personal entre las partes, mientras que el segundo se fundamenta en la tecnología de cadena de bloques que los sustenta. La supresión del requisito de la confianza entre los agentes de la transferencia informal¹⁸⁶ supone una ventaja estratégica para los grupos terroristas porque elimina la dependencia de redes neuronales que requieren de tiempo para forjarse y que son particularmente susceptibles a cambios y/o fallos; porque se pueden automatizar procesos con contratos inteligentes y porque facilita el acceso a zonas de conflicto o aislamiento. Otra diferencia evidente entre el *hawala* y los criptoactivos es la velocidad de transacción, siendo las criptomonedas una vía mucho más rápida de movilizar los fondos¹⁸⁷. A diferencia de aquel, el empleo de activos

¹⁸³ A. MICCOLI. *Hawala and cryptocurrencies: a new avenue for terrorist financing* [Trabajo de Fin de Máster, Luiss Guido Carli]. Biblioteca LuissThesis, 2023, págs. 73 y 74.

¹⁸⁴ A. MARZHA, U. ASSEM & L. KI-JOUNE. “Detecting Hawala network for money laundering by graph mining”. *The Journal of Finance and Data Science*, núm. 10, 2014, págs. 2 y 5.

¹⁸⁵ M. EL QORCHI; S. MUNZELE & J. WILSON. *Informal Funds Transfer Systems. An Analysis of the Informal Hawala System*. Fondo Monetario Internacional, 2003, pág. 14.

¹⁸⁶ C. RYUNG HAN & H. NELEN. “A living financial fossil, hawala: the evolution of informal fund transfer systems in Korea”. *Trends in Organized Crime*, vol. 28, núm. 1, 2025, pág. 19.

¹⁸⁷ En el trabajo de N. MEDRANDA & M. ARCOS. “Criptoactivos y criptomonedas”. *Blockchain, criptoactivos y metaverso. Una aproximación teórica*. Editorial Abya-Yala,

virtuales en el proceso financiador permite a los terroristas ahorrar el tiempo de coordinación entre intermediarios y de logística y movilidad. No obstante, también difieren en la naturaleza del registro y la trazabilidad de las operaciones. En el caso del *hawala*, los datos personales de las partes—especialmente de los clientes—se conservan temporalmente mientras dure la transacción, pero suelen destruirse una vez finalizada, logrando que la operación sea completamente opaca para las autoridades fiscales¹⁸⁸. Por su parte, las transacciones realizadas en *blockchain*, aunque preservan la privacidad y el anonimato de los sujetos intervenientes, quedan registradas de forma permanente e inmutable en una especie de libro contable público. Si bien no se revelan nombres, sí permite rastrear patrones de movimiento de fondos¹⁸⁹, ofreciendo una transparencia vinculada a actividades, aunque no a identidades.

De acuerdo con la exposición previa, se puede establecer la siguiente tabla comparativa entre el sistema *hawala* y las criptomonedas, dando especial atención a las dimensiones críticas para el análisis de riesgo y las ventajas tácticas para el uso ilícito:

Tabla 9: Comparación entre el sistema *hawala* y las criptomonedas como método de transferencia de fondos con fines ilícitos. Fuente: Elaboración propia

Dimensión/funcionalidad	Hawala	Criptoactivos/ Blockchain	Ventajas para el uso ilícito
Fundamento	Personal, comunitaria y basada en la reputación	Tecnológica, sin depender de terceros	Activos virtuales permiten operar sin vínculos personales subjetivos e inestables

2023, págs. 53 y 55; se ofrecen algunos datos interesantes: la creación de bloques en la cadena tiene una duración entre tres y cinco segundos y en Ethereum las transacciones se realizan en aproximadamente doce segundos.

¹⁸⁸ C. MALLADA. “La financiación del terrorismo desde la perspectiva de las nuevas tecnologías. A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo”. *Op. Cit.*, pág. 249.

¹⁸⁹ Salvo el caso de las criptomonedas privadas, que son muy difíciles de rastrear, tal como aclaran M. HARLEV, K. SUN YIN, K. LANGENHELDT, R. MUUKAMALA & R. VATRAPU. “Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning”. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018, pág. 3505; es posible agrupar datos de la cadena de bloques en *clústeres* y, al utilizar direcciones ya identificadas, agrupadas y categorizadas, predecir un *clúster* no identificado con amplio porcentaje de acierto. Además, indican los autores que el nivel de anonimato de *Bitcoin* es muy relativo, siendo posible reducir el número de posibles propietarios de una dirección criptográfica.

Dimensión/ funcionalidad	Hawala	Criptoactivos/ Blockchain	Ventajas para el uso ilícito
Supervisión/ regulación	Escasa o nula	Heterogénea, con especial atención a los prestadores de servicios con criptoactivos	Ambos esquemas permiten eludir controles, pero cripto-monedas son más adaptables a las necesidades de grupos criminales
Nivel de anonimato	Nivel muy alto, carece de registros formales	Nivel variable, dependiendo de la criptomoneda de que se trate y las técnicas forenses de trazabilidad	Criptoactivos ofrecen una privacidad/anonimato variable, pero no sujeto a conflictos y subjetividades humanas
Intermediación	Personal, con <i>hawaladars</i>	En general, funciona con nodos informáticos. Puede ser en P2P o automatizados	<i>Hawala</i> tiene más puntos de fricción y fallo humano
Alcance geográfico	Limitado a ciertas regiones y/o áreas geográficas	Global	Criptomonedas son más accesibles desde cualquier parte del mundo, solo se necesita un dispositivo con acceso a Internet
Trazabilidad	Nula si no hay colaboración y/o identificación del intermediario	Muy posible en cadenas de bloques públicas, pero con dificultades	<i>Hawala</i> ofrece mayor privacidad natural, pero depende de la confianza interpersonal con el consecuente riesgo de traición; criptomonedas son trazables, máxime con el trabajo activo actual para su regulación y vigilancia técnica

Dimensión/funcionalidad	Hawala	Criptoactivos/Blockchain	Ventajas para el uso ilícito
Fragmentación de fondos	Poco viable, se envían fondos acordados y suelen ser grandes cantidades	Muy viable, transacciones a múltiples <i>wallets</i> y transacciones pequeñas	Activos virtuales son particularmente efec-tivos para blanquear, evadir impuestos y hacer operaciones fraccio-nadas
Coordinación	Requiere contacto directo	Possible sin contacto directo	Criptomonedas permiten descentralización opera-tiva
Automatización	No se permiten procesos automá-ticos	Sí se permiten procesos automá-ticos, por ejemplo, <i>smart contracts</i>	Criptomonedas reducen errores humanos y aceleran las operaciones
Costo operativo	Bajo, especial-mente si es en zonas cercanas	Variable, depen-diendo de la red	Ambos son más económicos que el sistema bancario tradicional

3.6.2. Casos específicos de transmisión de bienes con fines terroristas

En general, las criptomonedas son susceptibles de abuso por parte de los terroristas, al permitir su transferencia a destinatarios globales¹⁹⁰. Por eso, es particularmente importante rastrear los flujos financieros cripto como estrategia de prevención, detección e investigación del terrorismo en general y otros delitos financieros¹⁹¹. No es de extrañar, entonces que los esfuerzos regulatorios se orienten en que los proveedores de servicios de pago y de custodia de criptoactivos establezcan sistemas y controles efectivos para detectar transferencias sospechosas y en controlar el tamaño de estas. Los grupos terroristas han adoptado las criptomonedas como herramienta para transferir fondos de manera rápida y, en apa-riencia, anónima, facilitando la financiación de sus actividades ilícitas. Por ejemplo, realizan transferencias directas entre billeteras digitales para distintos objetivos concretos, utilizan plataformas de intercambio de criptomonedas para convertir activos digitales en moneda *fiat* o para

¹⁹⁰ FINANCIAL INTELLIGENCE CENTRE. Assessment of the Money Laundering and Terrorist Financing Risk. Crypto Asset Service Providers, 1 de abril de 2025, pág. 25.

¹⁹¹ EUROPEAN BANKING AUTHORITY. Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. EBA/GL/2024/11, 4 de julio de 2024, pág. 35.

mover fondos entre diferentes criptomonedas, entre otras técnicas. AMIRAM et.al.¹⁹² entienden que hay dos tipos de transferencias en la financiación del terrorismo: las que realizan terceros a través de donaciones a largo plazo y las que realizan las organizaciones terroristas y sus miembros “en el terreno”. Se entiende que la segunda clasificación es la que se incardinaría en la conducta típica que se analiza, pues la primera, desde la posición de los terroristas, se adecuaría a “recabar” o “adquirir”.

Un caso destacable sobre la financiación del terrorismo tiene que ver con la utilización de pequeñas y medianas empresas como fachada para transferir fondos mediante activos digitales¹⁹³. Este enfoque imita estrategias comunes de *start-ups*, como la captación de fondos, las transferencias transfronterizas y el uso de plataformas tecnológicas, pero con fines ilícitos. Por ejemplo, estos criminales crean dichos negocios aceptando criptomonedas como medio de pago. Hamás se ha valido ampliamente de esta estrategia. En primer lugar, la plataforma de intercambio de criptomonedas Al Mutadahum fue incluida en la lista de organizaciones terroristas por transferir millones de dólares de Irán a Hamás¹⁹⁴, lo cual fue identificado con la utilización del sistema inteligente de rastreo de criptomonedas Chainalysis¹⁹⁵. Similar al caso anterior es el de la empre-

¹⁹² D. AMIRAM, B. JØRGENSEN & D. RABETTI. “Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks”. *Journal of Accounting Research*, Wiley Library, vol. 60, núm. 2, 2022, s/p. Versión electronica recuperada del siguiente enlace: <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-679X.12430>. Consultado por última vez el día 10 de julio de 2025.

¹⁹³ S. BRADY. “Assessing Opportunity and Innovation in Terrorist Financing in a Post Covid Environment”. En *Countering Terrorism Financing*. Centre of Excellence Defence Against Terrorism, Nicholas Ryder (edit.), 2022, pág. 20.

¹⁹⁴ M. WILLIAMSON. “Israeli Authorities Seize 30 Crypto Wallets Linked to Financing Terrorism”. *Finance Magnates*, 28 de febrero de 2022, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.financemagnates.com/cryptocurrency/israeli-authorities-seize-30-crypto-wallets-linked-to-financing-terrorism/>. Consultado por última vez el día 10 de julio de 2025.

¹⁹⁵ Chainalysis ofrece datos específicos sobre el caso, incluso enumera las direcciones públicas de criptoactivos involucradas con Hamás. La plataforma explica cómo ha sido posible: “Las autoridades israelíes analizaron OSINT para encontrar las direcciones de donación de Hamás y, con herramientas de análisis de blockchain, pudieron rastrear los fondos para encontrar direcciones de consolidación y descubrir los nombres de las personas asociadas con las campañas. Contar con datos actualizados de transacciones en varias blockchains fue crucial, ya que los agentes rastrearon e incautaron fondos en diversas criptomonedas”. CHAINALYSIS. “Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns”, 8 de julio de 2021, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.chainalysis.com/blog/israel-hamas-cryptocurrency-seizure-july-2021/>. Consultado por última vez el día 10 de julio de 2025. Las autoridades de Israel -cuya participación fue clave en la identificación e incautación de tales fondos- emitieron un informe donde constan otros datos similares, junto al nombre, número de identificación y correo electrónico de los responsables. Puede consultarse en el siguiente enlace: <https://nbcft.mod.gov.il/he/Announcements/Documents/%d60%d7%a6%d7%95%20%d7%aa%d7%a4%d7%99%d7%a1%d7%94%20%d7%9e%d7%99%d7%a0%d7%94%d7%9c%d7%99%2010.22.pdf>.

sa BTCTurk, sita en Estambul, a través de la cual se canalizaron fondos dirigidos a Hamás. En el informe de NORDIC MONITOR¹⁹⁶ se indica que el valor de los activos transferidos a la organización terrorista ascendió a más de un millón de dólares y advierte que “el sistema financiero turco podría estar permitiendo estos movimientos ilícitos de dinero a una escala alarmante”. Evidentemente, operar a través de empresas registradas propicia un rastro documental de sus actividades, aunado a la publicidad que brinda *blockchain*. No obstante, la dificultad radica en que estas entidades simulan operar de forma legítima y suelen operar en países con nivel bajo de intervención punitiva en materia de blanqueo de capitales y financiación del terrorismo, como lo ha sido Turquía.

Otro paradigma de este comportamiento típico es el uso de organizaciones aparentemente benéficas, como fundaciones¹⁹⁷, que han utilizado transferencias de criptomonedas para financiar el terrorismo. Por ejemplo, la organización Al-Sadaqah, que pretendía recaudar fondos para los combatientes de Siria con criptomonedas, ha apoyado proyectos relacionados con la yihad. De acuerdo con el informe de MEMRI¹⁹⁸, han complementado la privacidad de tales activos virtuales con el de otras tecnologías, como *Telegram* y la Internet profunda. Relacionado con lo anterior está el caso de Al Ikhwa, que se presentaba en su perfil de redes sociales —*Telegram*, en concreto— como una organización benéfica de Siria que no apoya ningún acto de terrorismo. Sin embargo, gracias al análisis inteligente de las cadenas de bloques y de las publicaciones disponibles en las redes sociales se constató que transferían “pagos anónimos” a organizaciones terroristas¹⁹⁹. Se aprecia el uso reiterado de plataformas de

¹⁹⁶ NORDIC MONITOR. “US Crackdown on Hamas virtual currency reveals Turkey’s role in terrorism financing”. FinCrime Central, s/f. Recurso electrónico recuperado del siguiente enlace: <https://fincrimecentral.com/us-crackdown-hamas-crypto-turkey-financing/>. Consultado por última vez el día 20 de mayo de 2025. Por su parte, A. BOZKURT. “U.S. Crackdown on Hamas Virtual Currency Sheds Light on Turkey’s Role in Terrorism Financing”. Middle East Forum, 3 de abril de 2025. Recurso electrónico recuperado del siguiente enlace: <https://www.meforum.org/mef-online/u-s-crackdown-on-hamas-virtual-currency-sheds-light-on-turkeys-role-in-terrorism-financing>. Consultado por última vez el día 10 de julio de 2025; indica que BTCTurk llegó a ser una de las plataformas de intercambio de criptomonedas más grandes de Europa y, sin duda, de Turquía. Además, ha operado con diversas entidades y empresas asociadas, lo que implica un entramado complejo de negocios.

¹⁹⁷ N. RYDER. “Terrorism financing and fraud – the unseen (seen) nexus?”. *Countering Terrorism Financing*. Centre of Excellence Defence Against Terrorism, Nicholas Ryder (edit.), 2022, pág. 169

¹⁹⁸ MEMRI. “A Review Of Al-Sadaqah Organization’s Activity On Telegram: Group Updates Its WhatsApp Number, Uses Deep Web-Based Email Service SecMail” [Nota de Prensa], agosto de 2018, s/p. Recurso electrónico recuperado del siguiente enlace: <https://www.memri.org/cjlab/a-review-of-al-sadaqah-organizations-activity-on-%C3%A2%C2%E2%82%AC%C5%BEtelegram-group-updates-its-whatsapp-number-uses-%C3%A2%C2%E2%82%AC%C5%BEdeep-web-based-email-service-secmail>. Consultado por última vez el día 10 de julio de 2025.

¹⁹⁹ Así ha sido expuesto en la denuncia verificada de Estados Unidos por decomiso *in rem*, núm. 1:20-cv-02228, documento 1, presentado el 13 de agosto de 2020, pág. 10.

mensajería cifrada por aparentes fundaciones, entre otras cosas ya mencionadas, por suponer una estrategia de reducción de costos, pues crean una imagen cercana y con una guía de estilo propia sin necesidad de invertir en páginas *webs* complejas que pueden ser fácilmente identificadas y cerradas por una orden judicial²⁰⁰.

3.7. Otras actividades

El legislador español ha optado por el uso de una cláusula analógica de cierre genérica en el delito de financiación del terrorismo. Este tipo de cláusulas, “especialmente objetables” para ROXIN²⁰¹, se suelen utilizar cuando no es posible determinar una amplia gama de variables conductuales que puedan perturbar el bien jurídico protegido por la norma penal²⁰². De hecho, el art. 576.4 CP supone interrogantes en lo que respecta a la dogmática penal, que se proyectan también en su comisión en el ámbito cripto. Por eso, es necesaria una superlativa cautela en su empleo, pues son técnicas legislativas capaces de generar situaciones de inseguridad jurídica. Al carecer de una delimitación precisa, puede conducir a interpretaciones excesivamente amplias por los Jueces y Tribunales²⁰³. No obstante, por la amplitud de conductas que ya menciona específicamente el tipo penal, es difícil de imaginar otros comportamientos

Recurso disponible en el siguiente enlace: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Criminal%20Complaint_Al-Ikhwa%20Accounts.pdf. Consultado por última vez el día 10 de julio de 2025.

²⁰⁰ De conformidad con A. ANDRIANOVA. “Countering the Financing of Terrorism in the Conditions of Digital Economy”. *Digital Transformation of the Economy: Challenges, Trends and New Opportunities*. Svetlana Ashmarina, Anabela Mesquita y Marek Vochozka (eds.). Advances in Intelligent Systems and Computing, vol. 908. Springer, 2020, pág. 23; “diversos canales de comunicación en línea, como redes sociales, canales cifrados de Telegram, mensajería instantánea, salas de chat y sitios web en la Darknet (el segmento oculto de Internet) permiten a los terroristas atraer a personas con ideas afines para expandir el apoyo, el flujo de efectivo y todo el flujo de recursos del mundo”.

²⁰¹ C. ROXIN. *Teoría del Tipo Penal. Tipos Abiertos y Elementos del Deber Jurídico*. Traducido al español por Enrique Bacigalupo. Ediciones Depalma, 1979, pág. 272.

²⁰² L. MÖMBLANC. “Legalidad versus tipos penales abiertos en el Código Penal cubano”. *Lex*, núm. 11, año 11, 2013, págs. 241 y 242. En relación con tal idea, *vid.* F. MUÑOZ CONDE & M. GARCÍA ARÁN. *Derecho Penal. Parte General*, 8^a Edición. Tirant Lo Blanch, 2010, pág. 257. En este Manual se indica que “es imposible llegar a describir exhaustivamente todas las formas de aparición de un delito (piénsese, por ejemplo, en la estafa) y, por ello, resulta preferible utilizar cláusulas generales, definiciones y descripciones genéricas que reúnan los caracteres comunes esenciales a cada grupo de delito”.

²⁰³ J. MIQUEL GÓNZÁLEZ. “Cláusulas generales y desarrollo judicial del Derecho”. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, núm. 1, 1997, págs. 297 y 298; considera que estas previsiones generales pueden dotar a los operadores jurídicos que se encargan de aplicar el Derecho de una vía para “modificar las leyes”, poniendo en riesgo la división de poderes.

factibles, tal como destaca NAVARRO CARDOSO²⁰⁴. Y esto es aplicable también a tal financiamiento con criptomonedas pues, como se ha visto a lo largo de este Capítulo, incluso conductas propias de los tecnicismos de estos activos, como la minería, están perfectamente abarcadas en los verbos rectores expresamente indicados por el legislador.

4. Elementos subjetivos del delito de financiación del terrorismo en el contexto cripto

El delito de financiación del terrorismo, según la configuración típica del art. 576.1 CP, incluye un elemento subjetivo del injusto: la intención o el conocimiento de que los fondos en cuestión serán utilizados total o parcialmente con fines terroristas. A nivel doctrinal se entiende que basta con que se constate que el autor sepa o quiera que el tratamiento de los bienes persigue ese objetivo²⁰⁵. Tomando esta exigencia típica en consideración, NAVARRO CARDOSO²⁰⁶ afirma que se produce una exclusión del dolo eventual y se hace necesario probar la concurrencia de tales elementos para que de lugar a responsabilidad penal. Aunque esto no se corresponde con la línea jurisprudencial asentada en materia de comportamientos de colaboración terrorista, donde se sostiene que la aceptación del riesgo (dolo eventual) puede derivar en responsabilidad penal²⁰⁷ y “no es preciso ningún elemento subjetivo del injusto más allá de los propios de toda conducta dolosa: conocimiento y voluntad”²⁰⁸. Pero esto puede ser altamente complejo en el caso de un tipo delictivo al que se le otorga naturaleza preparatoria y abarca un numero amplio e indeterminados de delitos-fin, como el finamiento terrorista²⁰⁹. Parece que, en la práctica, solo ha de confirmarse que quien interviene en el acto de financiación puede y debe saber que su aporte servirá como medio para cumplir objetivos criminales.

²⁰⁴ F. NAVARRO CARDOSO. “Los tipos dolosos del delito de financiación del terrorismo”. *Op. Cit.*, pág. 9.

²⁰⁵ E. AGUDO FERNÁNDEZ, M. JAÉN VALLEJO & Á. PERRINO PÉREZ. *Terrorismo en el siglo XXI (La respuesta penal en el escenario mundial)*. Editorial Dykinson, 2016, pág. 144.

²⁰⁶ F. NAVARRO CARDOSO, F. “Los tipos dolosos del delito de financiación del terrorismo”. *Op. Cit.*, pág. 17.

²⁰⁷ A modo de ejemplo, *vid.* STS 439/2014, 10 de Julio de 2014, FJ 14.

²⁰⁸ STS 797/2005, FJ 4. En ilación, la STS 540/2010, FJ 5, indica que los fines específicos del colaborador -o, en este caso, sujeto que interviene en el proceso de financiación- con grupo terrorista no es relevante, “pues lo que aquí se sanciona no es la adhesión ideológica ni la prosecución de determinados objetivos políticos o ideológicos, sino el poner a disposición de la banda armada determinadas aportaciones, conociendo que los medios y métodos empleados por la organización consisten en hacer uso de la violencia, es decir, del terror y de la muerte, cuando en un Estado Social y Democrático de Derecho, como el nuestro, existen cauces pacíficos y democráticos para la prosecución de cualquier finalidad política”.

²⁰⁹ A. ALONSO RIMO. *El tipo subjetivo de los actos preparatorios del delito*. Editorial Tirant Lo Blanch, 1^a Edición, 2023, pág. 20.

En el caso de la financiación del terrorismo con criptomonedas, es crucial valorar la concreción del elemento subjetivo del injusto ya comentado en función del contexto tecnológico, sin olvidar las garantías propias del Derecho penal. Es cierto que la privacidad o el anonimato que ofrecen los activos virtuales dificultan probar la intención o conocimiento concreto del destino terrorista. Además, al producirse todo el proceso de financiación en la red, la mayoría o los únicos puntos de contacto indiciario existen en ese entorno²¹⁰. Esto requiere análisis forenses digitales especializados basados en sistemas inteligentes de rastreo que únicamente establecen grafos de conexiones entre nodos. Por tanto, para confirmar que existe conocimiento o aceptación del riesgo delictivo, los operadores judiciales tendrían que valorar e interpretar información adicional sobre esas relaciones digitales. Atendiendo a los criterios técnicos de trazabilidad y a los criterios jurídicos de imputación subjetiva, el análisis del tipo subjetivo no debería centrarse en la mera existencia de una conexión entre *wallets*, sino en indicios razonables de que perseguía favorecer económicamente el terrorismo. Así, por ejemplo, se puede tomar en cuenta si el emisor ha realizado aportaciones a cuentas que han sido vinculadas con actividades terroristas; si ha usado *mixers* y/o criptomonedas privadas que no son ampliamente utilizadas por la comunidad cripto en su conjunto; si estaba apoyando una campaña de *crowdfunding* o un proyecto caritativo con apariencia de legalidad; si ha participado en foros, canales digitales o grupos en redes sociales relacionados con ideologías extremistas; si ha contactado con los destinatarios de los fondos en la Internet profunda o a través de sistemas de cifrado; etc. Un elemento útil en este sentido son los oráculos²¹¹, que favorecen el suministro de datos entre un sistema *blockchain* y sistemas externos²¹².

²¹⁰ Esto rememora la apreciación de C. MALLADA FERNÁNDEZ. “La financiación del terrorismo desde la perspectiva de las nuevas tecnologías. A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo”. *Op. Cit.*, pág. 244; quien afirma que la ciberdelincuencia, en general, produce una desmaterialización del producto del delito que aleja al delincuente físicamente de los beneficios económicos obtenidos. Esto dificulta su rastreo en comparación con la delincuencia tradicional y obliga a las Fuerzas y Cuerpos de Seguridad del Estado a enfocarse en otros aspectos del delito porque, en algún punto, se dejará un rastro.

²¹¹ En este sentido, varios investigadores italianos proponen un oráculo implementado en *Python* -un lenguaje de programación- con tres componentes: a) lenguaje de consulta; b) intérprete, que analiza e interpreta las consultas y; c) cliente, que recupera los datos reales de las *blockchain* públicas. Este sistema permite evaluar propiedades temporales complejas a lo largo del tiempo y, en consecuencia, detectar tendencias, anomalías y comportamientos emergentes dentro de las transacciones en la cadena de bloques. M. BLANCHINI, et.al. “Supporting Criminal Investigations on the Blockchain: A Temporal Logic-based Approach”. *ITASEC 2024: The Italian Conference on CyberSecurity*, CEUR Workshop Proceedings, 2024, págs. 6 y 7.

²¹² R. HUMPHRY, P. AVRAMOVIC, F. ACEVEDO, S. ALKHAIR & A. GERVAIS. Review of Maximal Extractable Value & Blockchain Oracles. Research Note, FCA, 2024, pág. 17.

Ha existido debate sobre la asunción del contenido de la cadena de bloques como medio válido para esclarecer los hechos en un proceso penal. En España, no obstante, el TS ya ha aclarado que los correos electrónicos, respaldos de operaciones cripto con los códigos de identificación inherentes y otra documentación relacionada son piezas de convicción en función de su coherencia y compatibilidad con el resto de material acreditativo presentado, así como el resultado de informes periciales²¹³. Por otra parte, recopilar toda la información descrita no es tarea fácil, ya que la mayoría de las veces tal material probatorio está diseminado en distintas jurisdicciones. A nivel supranacional, en la Unión Europea, se ha promovido el intercambio transfronterizo de información a través de sistemas informáticos descentralizados —como es *blockchain*— para reforzar la cooperación judicial y se ha ido perfilando progresivamente la Orden Europea de Investigación, en los términos expresados en la Directiva 2014/41/CE del Parlamento Europeo y del Consejo. En cuanto a este último instrumento, definida en el art. 1.1 de la norma como “una resolución judicial emitida o validada por una autoridad judicial de un Estado miembro («el Estado de emisión») para llevar a cabo una o varias medidas de investigación en otro Estado miembro («el Estado de ejecución») con vistas a obtener pruebas con arreglo a la presente Directiva”, permite a la autoridad competente de un Estado solicitar una actuación que recaiga sobre determinados datos en soporte electrónico directamente a un prestador de servicios que los tiene almacenados²¹⁴, que bien podría ser un prestador de servicios de activos virtuales. Además, la mencionada Orden se convierte en el mecanismo ideal para solicitar a otro Estado miembro que lleve a cabo alguna de las siguientes medidas de investigación tecnológica, en el marco de una investigación donde medien criptomonedas: la interceptación de comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante dispositivos electrónicos, registro de dispositivos de almacenamiento masivo de información y de otros sistemas desde el dispositivo central y los registros remotos sobre equipos informáticos²¹⁵.

²¹³ STS 326/2019, FJ 1. En opinión de J. CRIADO ENGUIX. “Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito”. *Revista de Estudios Europeos*, núm. 85, 2025, pág. 514; *Blockchain* valida y registra transacciones que han tenido lugar de forma irrevocable a lo largo del tiempo, por lo que constituye una forma de documento electrónico, de conformidad con lo expuesto en el art. 26 CP y el art. 743.1 LEcRim.

²¹⁴ J. DELGADO MARTÍN. “Prueba digital internacional. El Reglamento E-Evidence”. *Diario La Ley*, núm. 76, 2023, pág. 6. De hecho, el Considerando 64 de la Directiva identificada indica que la configuración de los programas informáticos realizados debe permitir a los Estados miembros potenciar su infraestructura nacional de comunicación judicial para fines de uso transfronterizo.

²¹⁵ F. ORDÓÑEZ PONZ. “Investigación y cooperación judicial en los delitos en los que intervengan criptomonedas”. *Cooperación judicial civil y penal en la Unión Europea. Retos pendientes y nuevos desafíos ante la transformación digital del proceso*, Paulo Suárez y Ana María Vicario (dirs.). Editorial Bosch Procesal, 2023, págs. 114, 122 y ss.

Las herramientas de investigación de movimientos de activos virtuales se basan en dos técnicas de recopilación de datos. La primera es el agrupamiento de direcciones a partir de modelos heurísticos, con el fin de asignar subconjuntos máximos (también llamados clústeres) a un actor del mundo real. La segunda son las etiquetas de atribución, entendidas como cualquier información contextual que se pueda atribuir a una dirección, transacción o clúster, con especial interés en información de identificación personal del titular de la cuenta²¹⁶. En el trabajo de KUMAR et. al.²¹⁷ se demuestra que, mientras más grande es el tamaño de una agrupación de datos o clúster, mayor es la posibilidad de que se puedan trazar los movimientos. Por tanto, para demostrar tanto factores objetivos como subjetivos de un delito basado en criptomonedas, es necesario emplear una combinación de técnicas forenses digitales especializadas²¹⁸. Así, se reiteran las palabras de HINOJAL²¹⁹ cuando afirma que es necesario invertir en el desarrollo de herramientas y técnicas avanzadas de análisis de cadena de bloques y contar con expertos capacitados para interpretar esos datos.

5. Conclusiones

El terrorismo es un fenómeno en auge y de difícil abordaje por su carácter multidimensional. Abarca cuantiosos comportamientos y amenazas caracterizados por la violencia y por los incontables riesgos que supone para la seguridad a nivel global. La materialización de estos ataques y el funcionamiento de las organizaciones y redes terroristas depende, en

²¹⁶ M. FRÖWIS, et. al. "Safeguarding the evidential value of forensic cryptocurrency investigations". *Forensic Science International: Digital Investigation*, núm. 33, 2020, págs. 1 y 2.

²¹⁷ A. KUMAR, et.al. "A Traceability Analysis of Monero's Blockchain". *Computer Security – ESORICS 2017*, 22nd European Symposium on Research in Computer Security Oslo, Norway, September 11–15, 2017, Proceedings, Parte 2. Simon Foley, Dieter Gollmann y Einar Snekkenes (eds.), Springer, 2017, págs. 156 y ss. Los autores prueban una serie de ataques de trazabilidad, identificando los pasos y resultados obtenidos. Incluso, demuestran la relación entre el tamaño de los datos y la probabilidad de rastreo en los casos en que se utilizan *mixers* para potenciar la privacidad y/o anonimato. En las conclusiones indican que aún hay que seguir trabajando en técnicas de trazabilidad para las transacciones con Monero.

²¹⁸ Para autores como A. MAJUMDER, M. ROUTH & D. SINGHA. "A conceptual study on the emergence of cryptocurrency economy and its nexus with terrorism financing". *The impact of global terrorism on economic and political development*, Ramesh Chandra (edit.). Editorial Emerald Publishing, 2019, pág. 137; la mera elección de criptomonedas para hacer una transacción de activos es evidencia de que se trata de una acción ilegal pues, si se persiguiese un fin legítimo, el autor del movimiento optaría por una vía rastreable y con mayor soporte legal. Pero esto, como se puede inferir de lo ya señalado en este trabajo, concueraría directamente con la presunción de inocencia y principios básicos de un Derecho penal democrático, como el de legalidad.

²¹⁹ A. HINOJAL. "Criptomonedas y blanqueo de capitales". En Lógos: *Revista Científica del Centro Universitario de la guardia Civil*, 2023, pág. 234.

gran medida, de los medios que tengan a su alcance. De ahí que atender la financiación del terrorismo sea una cuestión innegociable para las jurisdicciones comprometidas con la defensa de los derechos humanos, la democracia y la protección de la comunidad. Para ello, hay importantes directrices y recomendaciones emitidas por organismos internacionales de gran calado como el GAFI. La idea central de la mayoría de las políticas en materia de financiamiento terrorista es la prevención y un enfoque basado en el riesgo puesto que, una vez que se ejecuta la movilización de fondos es difícil controlar que eso no desemboque en un atentado o el perfeccionamiento estructural y operativo de los terroristas. Además, se propicia una cultura compartida jurídico-penal, con la tipificación de la financiación del terrorismo como delito autónomo.

En España, el delito de financiación del terrorismo se halla en el art. 576 CP, castigando a quien/es realice/n alguna/s de las varias conductas típicas recogidas por el legislador. Esta técnica legislativa es coincidente, como se ha comentado, con la de muchos otros Estados a nivel mundial. La intención es abarcar tanto como sea posible para que la capacidad transformadora del terrorismo no ponga en jaque la vigencia y eficacia de la norma penal. Esto, a su vez, ha dado lugar a un amplio debate sobre si es una manifestación mas del expansionismo del Derecho penal, con los riesgos democráticos y de seguridad jurídica que eso supone. Sin embargo, la realidad es que la regulación actual ha permitido sortear los cambios que ha propiciado la llegada de las nuevas tecnologías para financiar las actividades terroristas. De hecho, la configuración típica del art. 576 CP incluye el terrorismo cibernético, tanto directa como indirectamente. Al definir como objeto material del delito a “bienes o valores de cualquier clase”, no cabe duda de que el legislador permite asimilar como tal a las criptomonedas.

Analizando cada una de las conductas típicas del delito de financiamento terrorista, se ha podido comprobar que, tanto en la teoría como en la práctica, está absolutamente comprobada su perpetración con la intervención de criptoactivos. El financiamiento del terrorismo mediante criptoactivos abarca una variedad de conductas típicas claramente verificables tanto en la teoría como en la práctica. Los terroristas pueden recaudar fondos a través de crowdfunding, minería (incluso ilícita) y empresas pantalla; adquirirlos mediante la venta de bienes y servicios ilícitos en la Dark Web o con la emisión de NFTs; poseerlos controlando directamente las claves de wallets o influyendo sobre comunidades cripto; utilizarlos para comprar armas, servicios ilegales o financiar propaganda; convertirlos en otros activos usando exchanges, cajeros o tokens, incluso con asistencia o automatización tecnológica; y transmitirlos dentro o fuera del sistema financiero formal, recurriendo a métodos como el sistema hawala o combinándolos con criptomonedas según sus necesidades estratégicas. Esta flexibilidad operativa, unida a la descentralización y al bajo nivel de supervisión, convierte a los criptoactivos en herramientas particularmente atractivas para el terrorismo contemporáneo.

Durante el estudio de las conductas que integran el delito de financiamiento terrorista y sus proyecciones prácticas se ha podido comprobar que múltiples estudios recientes proponen herramientas técnicas y programas informáticos para investigar estos supuestos e identificar a los responsables. Por ejemplo, los detectores de minería ilícita basados en tecnologías de aprendizaje automático, el análisis del IP y el caché y las cookies para obtener datos forenses de billeteras criptográficas basadas en extensiones del navegador, la reconstrucción automática de eventos, uso de IA para análisis contextual de textos y reconocimiento de patrones comunes en redes sociales, entre otros. Ante la observancia de fenómenos criminales tecnológicos cuya detección requiere el empleo de sistemas sofisticados, los investigadores, cuerpos policiales y autoridades judiciales tienen la responsabilidad de familiarizarse con estos nuevos métodos y los Estados de realizar importantes inversiones en equipamiento especializado. En el caso de la financiación del terrorismo no es válido el argumento de que el volumen de transacciones ilícitas es ínfimo y por tanto no se justifica dicho nivel de inversión, pues la detección de flujos financieros vinculados a actividades terroristas no solo permite rastrear y desarticular redes de financiamiento, sino que también posibilita la identificación de sus responsables, constituyendo así una herramienta esencial en la lucha integral y estratégica contra el terrorismo.

El delito de financiación del terrorismo, tanto en la tipificación española como en las exigencias internacionales al respecto, incluye la intención o conocimiento de que los fondos serán utilizados total o parcialmente con fines terroristas como elemento subjetivo del injusto. El problema de probar este componente se agudiza con la intervención de las criptomonedas y la opacidad que propician. Por cuestiones de seguridad jurídica y de respeto por las demandas de un Derecho penal democrático no debería bastar la existencia de una conexión entre criptobilleteras para probar la comisión de tal delito. Es necesario determinar indicios razonables de que el autor o los autores perseguían ese resultado o, al menos, eran conscientes de el. Para ello, es necesario emplear una combinación de técnicas forenses digitales especializadas; máxime en el caso de las criptomonedas que solo existen y coexisten en la red. En España, el Tribunal Supremo ha reconocido la validez probatoria de elementos como correos electrónicos o respaldos de operaciones cripto, junto a informes periciales. Además, a nivel de la Unión Europea, la Orden Europea de Investigación prevista en la Directiva 2014/41/CE, permite solicitar medidas de investigación tecnológica en otros Estados miembros, lo cual resulta fundamental en este supuesto pues las pruebas suelen estar diseminadas en otras jurisdicciones.

6. Referencias consultadas

Referencias bibliográficas

ABDULLAIEVA, E. & GALCHYNSKY, L. "An Algorithm for Analyzing the Ethereum Network Blockchain to Detect Illegal Activities". *Theoretical and Applied Cyber Security*, vol. 6, núm. 1, 2024.

ABEL SOUTO, M. "Las reformas penales de 2015 sobre el blanqueo de dinero". *Revista Electrónica de Ciencia Penal y Criminología*, núm. 19-31, 2017.

ACALE SÁNCHEZ, M. "Terrorismo y tratamiento punitivista: más allá de la prisión". *El terrorismo en la actualidad: un nuevo enfoque político criminal*, Ana Pérez Cepeda (dir.). Editorial Tirant Lo Blanch, 2018.

AGUDO FERNÁNDEZ, E.; JAÉN VALLEJO, M. & PERRINO PÉREZ, Á. *Terrorismo en el siglo XXI (La respuesta penal en el escenario mundial)*. Editorial Dykinson, 2016.

ALI IBRAHIM, S. "Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing". *Pakistan Horizon*, vol. 74, núm. 1, 2021.

ALONSO RIMO, A. *El tipo subjetivo de los actos preparatorios del delito*. Editorial Tirant Lo Blanch, 1^a Edición, 2023.

ALONSO, Y. "La posición de la Unión Europea tras el 11-S. Revisión 'normativa' sobre prevención y cooperación frente al terrorismo". *Comillas Journal of International Relations*, núm. 26, 2023.

ÁLVAREZ LEÓN, J. & GARCÍA ASTUDILLO, F. "La no renovación de la clase gobernante y la cifra dorada. Una visión criminológica de la impunidad en México". *Revista del Posgrado en Derecho de la UNAM*.

AMIRAM, D.; JØRGENSEN, B. & RABETTI, D. "Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks". *Journal of Accounting Research*, Wiley Library, vol. 60, núm. 2, 2022.

ANDRIANOVA, A. "Countering the Financing of Terrorism in the Conditions of Digital Economy". *Digital Transformation of the Economy: Challenges, Trends and New Opportunities*. Svetlana Ashmarina, Ana-bela Mesquita y Marek Vochozka (eds.). *Advances in Intelligent Systems and Computing*, vol. 908. Springer, 2020.

ANGGRIAWAN, R & ENDRIYO, M. "Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations". *Novum Jus*, vol. 18, núm. 2, 2024.

ANTÚÑEZ, M. *La financiación del terrorismo internacional y su incidencia en la seguridad y la defensa*. Editor Ministerio de Defensa. Secretaría General Técnica, 2024.

ARGOMANIZ, J. "Post-9/11 institutionalisation of European Union counter-terrorism: emergence, acceleration and inertia". *European Security*, vol. 18, núm. 2, 2009.

ARIAS, R. & MANZANO, L. "El terrorismo y su transformación". *Revista Academia de Guerra del Ejército Ecuatoriano*, vol. 16, núm. 1, 2023.

ARISTEGUI, G. "El nuevo terrorismo". En *Cuenta y razón del pensamiento actual*, núm. 126, 2002.

ARMOUR, J. & ENRIQUES, L. "Individual investors' Access to Crowdfunding: Two regulatory models". *The Economics of Crowdfunding*, 2018.

BARÓN QUINTERO, S. "Los delitos realizados mediante la Dark Net". *Revista Penal México*, núm. 23, 2023.

BARRETT, R. "Preventing the financing of terrorism". *Journal of International Law*, vol. 44, núm. 3, 2012.

BEDECARRATZ. "Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal". *Revista Chilena de Derecho y Tecnología*, vol. 7, núm. 1, 2018.

BECERRA-MUÑOZ, J. & GARCÍA AGUILAR, D. "La política criminal antiterrorista en los tribunales". *Boletín Criminológico*, núm. 5, 2018.

BERNARDINO, S.; FREITAS, J. & CADIMA, J. "Social crowdfunding: A new model for financing regional development?". *Journal of Urban and Regional Analysis*, vol. 8, núm. 2, 2016.

BLANCHINI, M.; CERRETA, M.; DI MONDA, D.; FABBRI, M.; RACITI, M.; AHMAD, H. & COSTA, G. "Supporting Criminal Investigations on the Blockchain: A Temporal Logic-based Approach". *ITASEC 2024: The Italian Conference on CyberSecurity*, CEUR Workshop Proceedings, 2024.

BLANCO CORDERO, I. "¿Es necesario tipificar el delito de financiación del terrorismo en el Código Penal español?". *Athena Intelligence Journal*, vol. 4, núm. 1, 2009.

BOM CAMARGO, Y. "El Crowdfunding, una nueva oportunidad de financiamiento en América Latina y en el Caribe". *Opción*, año 34, núm. 18, 2018.

BORJA, E. "Justicia penal preventiva y Derecho penal de la globalización: proyecciones en el ámbito del terrorismo". En *Anuario de Derecho Penal y Ciencias Penales*, núm. 70, 2017.

BOVE, V.; EFTHYVOULOU, G.; GHAZARYAN, A. & PICKARD, H. "The emotional effect of terrorism". *Scientific Reports*, núm. 14, 2024.

BRADY, S. "Assessing Opportunity and Innovation in Terrorist Financing in a Post Covid Environment". En *Countering Terrorism Financing*. Centre of Excellence Defence Against Terrorism, Nicholas Ryder (edit.), 2022.

BUESA, M. "Financiación del terrorismo". *Economía del Terrorismo*, núm. 893, noviembre-diciembre, 2016.

BURGESS, A.; HAMILTON, R. & LEUPRECHT, C. "Terror on the Blockchain: The emergent crypto-crime-terror nexus". *Financial Crime, Law and Governance. Navigating Challenges in Different Contexts*. Ius Gentium: Comparative Perspectives on Law and Justice, vol. 116, Doron Goldbarsht y Louis de Koker (eds.). Springer, 2024.

CANCIO MELIÁ, M. *Los delitos de terrorismo: Estructura típica e injusto*. Editorial Reus, 2010.

CANO PAÑOS, M. "La reforma de los delitos de terrorismo". *Estudios sobre el Código Penal Reformado (Leyes Orgánicas 1/2015 y 2/2015)*. Lorenzo Morillas (dir.). Editorial Dykinson, 2015.

CARROLL, P. & WINDLE, J. "Cyber as an enabler of terrorism financing, now and in the future". *Journal of Policing, Intelligence and Counter Terrorism*, núm. 13-3, 2018.

CHATZIGIANNIS, P. & CHALKIAS, K. "Proof of Assets in the Diem Blockchain". *Applied Cryptography and Network Security Workshops*. ACNS 2021 Satellite Workshops AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA Kamakura, Japan, June 21–24, 2021, Proceedings. Jianying Zhou et.al (eds.). Springer, 2021.

CHIBUEZE, S. "Overview of Terrorist Financing in Nigeria: Legal and Institutional Framework for Combating Terrorism Financing". *SSRN Papers*, 2024.

CHIN-HUANG, L; LIOU, D. & WEI WU, K. "Opportunities and challenges created by terrorism". *Technological Forecasting and Social Change*, vol. 74, núm. 2, 2007.

CHOHAN, U. "A history of Bitcoin". En *Critical Blockchain Research Initiative, Discussion Paper Series: Notes on the 21st Century*, 2022.

CHRISTIN, N. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace". *22nd International Conference*, s/n, 2013.

CLAVIJO, J. *La prevención de blanqueo de capitales. Un análisis teórico-práctico*. J.M. Bosch Editor, 2022.

CRİADO ENGUIX, J. "Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito". *Revista de Estudios Europeos*, núm. 85, 2025.

DAVIS, J. "The Financial Future of the Islamic State". En *CTC Sentinel*, vol. 17, núm. 7, 2024.

DE GOEDE, M. "Hawala discourses and the war on terrorist finance". *Environment and Planning D: Society and Space*, vol. 21, 2003.

DE LA CORTE IBÁÑEZ, L. *La lógica del terrorismo*. Alianza Editorial, 2006.

DEL CARPIO, J. "El objeto material del blanqueo de capitales en la Directiva 2018/1673: a la vez, sobre la necesidad o no de modificar el

Código penal para dar cabida a las nuevas formas en las que puede representarse". *Revista Electrónica de Ciencia Penal y Criminología*, núm. 25, 2023.

DELGADO MARTÍN, J. "Prueba digital internacional. El Reglamento E-Evidence". *Diario La Ley*, núm. 76, 2023.

DÍAZ BERNARDOS, A. "Explorando las huellas digitales de los criptoactivos mediante fuentes abiertas". *Ciencia Policial*, núm. 182, 2024.

DIÓN-SCHWARZ, D.; MANHEIM, D. & JOHNSTON, P. *Terrorist Use of Cryptocurrencies*, National Security Research Division, 2019.

DÓMINE, M. "Criminalidad económica y terrorismo". *Revista de Derecho: Publicación de la Facultad de Derecho de la Universidad Católica de Uruguay*, núm. 1, 2006.

EL QORCHI, M.; MUNZELE, S. & WILSON, J. *Informal Funds Transfer Systems. An Analysis of the Informal Hawala System*. Fondo Monetario Internacional, 2003.

EL-QORCHI, M. "Hawala". *Finanzas y Desarrollo*, diciembre de 2022.

ESCUCHURI, E. & RUEDA MARTÍN, M. "Delitos contra el orden público II. Organizaciones y grupos criminales. Organizaciones y grupos terroristas y los delitos de terrorismo". *Derecho Penal, Parte Especial*. Carlos Romeo y Miguel Ángel Boldova (coords.). Editorial Comares, 2^a ed, 2022. Se advierte que esta obra tiene publicada una 3^a ed.

FAITH, D. "The Hawala System". *Global Security Studies*, vol. 2, núm. 1, 2011

FARBER, S. & YEHEZKEL, S. "Financial Extremism: The Dark Side of Crowdfunding and Terrorism". *Terrorism and Political Violence*, 2024.

FERRÉ OLIVÉ, J. "Aspectos conflictivos del delito de lavado de dinero". *Silver Anniversary Book Commemorating the 25th Anniversary of the Faculty of Law and Administration*. Uczelnia Łazarskiego, Stefański (ed.), 2022.

FETSYAK, I. "Consideraciones sobre la prevención del blanqueo de capitales y financiación del terrorismo mediante los tokens no fungibles (NFT)". *REDUR*, núm. 20, 2022.

FLETCHER, E.; LARKIN, C. & CORBET, S. "Countering money laundering and terrorist financing: A case for bitcoin regulation". *Research in International Business and Finance*, vol. 56, 2021.

FORTNOW, M. & TERRY, Q. *The NFT Handbook. How to create, sell and buy non-fungible tokens*. 1^a Edición, Editorial Wiley, 2022.

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

FRÖWIS, M.; GOTTSCHALK, T.; HASLHOFER, B.; RÜCKERT, C. & PESCH, P. "Safeguarding the evidential value of forensic cryptocurrency inves-

tigations". *Forensic Science International: Digital Investigation*, núm. 33, 2020.

GADEA, G. "El terrorismo, las nuevas tecnologías y la libertad de expresión en España". *Revista Pensamiento Penal*, núm. 12, 2015.

GADEA ALDAVE, G. "La política criminal de la Unión Europea con relación al terrorismo yihadista en internet" [Tesis de doctorado no publicada]. Universidad de Granada, 2024.

GARCÍA SIGMAN, L. "Narcotráfico en la Darkweb: los criptomercados". *URVIO Revista Latinoamericana de Estudios de Seguridad*, núm. 21, 2017.

GESLEVICH, N. & VOLOVELSKY, U. "Digital assets, anti-money laundering and counter financing of terrorism: An analysis of evolving regulations and enforcement in the era of NFTs". *The Cambridge Handbook on Law and Policy for NFTs*, Forthcoming, 2023.

GOLDBARSHT, D. "Dancing in the Dark: Terrorist Financing Via the Dark Web". *Financial Crime and the Law*, Doron Goldbarsht y Louis de Koker (eds.). Springer, 2024.

GONZÁLEZ CUSSAC, J. & VIDALES RODRÍGUEZ, C. "El nuevo delito de financiación del terrorismo: consideraciones acerca de su necesidad y conveniencia". *Financiación del terrorismo, blanqueo de capitales y secreto bancario: un análisis crítico*. José Luis González Cussac (dir.). Editorial Tirant Lo Blanch, 2009.

HARLEV, M.; SUN YIN, K.; LANGENHELDT, K.; MUKKAMALA, R. & VATRAPU, R. "Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning". *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

HINOJAL, A. "Criptomonedas y blanqueo de capitales". En Lógos: *Revista Científica del Centro Universitario de la guardia Civil*, 2023.

HINOJOSA, L. *La financiación del terrorismo y las Naciones Unidas*. Editorial Tecnos, 2008.

IRWIN, A. & TURNER, A. "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where". *Journal of Money Laundering Control*, vol. 21, núm. 3, 2018.

JAMWAL, N. "Hawala-The Invisible Financing System of Terrorism". *Strategic Analysis*, vol. 26, núm 2, 2022.

JOHANNES TEICHMANN, F. "Financing terrorism through cryptocurrencies – a danger for Europe?". *Journal of Money Laundering Control*, vol. 21, núm. 4, 2018.

JOHNSON, J. & JENSEN, C. "The financing of terrorism". *The Journal of the Institute of Justice & International Studies*, núm. 1, 2010.

JORDÁ, C.; PÍRIZ, C. & GIMÉNEZ-SALINAS, A. "Los criptomercados ilícitos de tráfico de drogas en la DarkWeb: un estudio exploratorio empírico".

co". *Revista Española de Investigación Criminológica*, vol. 22, núm. 2, 2024.

KAUNERT, C. & LEONARD, S. "The collective securitisation of terrorism in the European Union". *West European Politics*, vol. 42, núm. 2, 2020.

KIM, J.; SEO, S.; SEOK, B.; BUYN, H.; LEE, C.; JOO-EUN, K.; SEUNG-HEE, S.; BYEONG-JIN, S.; HYEON-SU, B. & CHANG, L. "A Study on the Digital Forensics Artifacts Collection and Analysis of Browser Extension-Based Crypto Wallet". *Journal of the Korea Institute of Information Security & Cryptology*, vol. 33, núm. 3, 2023.

KOH, W. "Terrorism and its impact on economic growth and technological innovation". *Technological Forecasting and Social Change*, vol. 74, núm. 2, 2007.

KUMAR, A.; FISCHER, C.; TOPLE, S. & SAXENA, P. "A Traceability Analysis of Monero's Blockchain". *Computer Security – ESORICS 2017*, 22nd European Symposium on Research in Computer Security Oslo, Norway, September 11–15, 2017, Proceedings, Parte 2. Simon Foley, Dieter Gollmann y Einar Snekkenes (eds.), Springer, 2017.

LAMARCA PÉREZ, C. "Sobre el concepto de terrorismo (A propósito del caso Amedo)". En *Anuario de Derecho Penal y Ciencias Penales*, tomo 46, fasc. 2, 1993.

LAURENCE, T. & KIM, S. "Developing Your Knowledge: A Step-by-Step Guide to Programming Your Own NFT". *NFTs For Dummies*. 1^a Edición, Editorial Wiley, 2021.

LI, C. & SHEN, Y. "The potential impacts and risks of global stablecoins". *China Economic Journal*, vol. 14, núm. 1, 2021

LI, Z.; LIU, W.; CHEN, H.; WANG, X.; LIAO, X.; XING, L.; ZHA, M.; JIN, H. & ZOU, D. "Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms". *IEEE Symposium on Security and Privacy (SP)*, 2022.

LISSOWSKA, M. "La regulación europea del crowdfunding: situación actual y desarrollos recientes". *Aspectos legales de la financiación en masa o crowdfunding*. Editorial Tirant Lo Blanch. Matilde Cuena (dir), 2020.

LOBERT JONES, B. "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road". *International Journal of Cyber Criminology*, vol. 10, núm. 1, 2016.

LODEIRO, R. "El uso de las nuevas tecnologías por el terrorismo yihadista". *Cuadernos de la Guardia Civil: Revista de Seguridad Pública*, núm. 54, 2017.

LÓPEZ CALERA, N. "El concepto de terrorismo. ¿Qué terrorismo? ¿Por qué el terrorismo? ¿Hasta cuándo el terrorismo?". En *Anuario de Filosofía del Derecho*, núm. 19, 2002.

MAJUMDER, A.; ROUTH, M. & SINGHA, D. "A conceptual study on the emergence of cryptocurrency economy and its nexus with terrorism financing". *The impact of global terrorism on economic and political development*, Ramesh Chandra (edit.). Editorial Emerald Publishing, 2019.

MALIK, N. *Terror in the dark. How terrorists use encryption, the Darknet, and Cryptocurrencies*. The Henry Jackson Society, 2018.

MANGGARANI, C. & AHMAD, Z. "The Determining Factors of Student Intention to Donate in Social Crowdfunding Media". *Hasanuddin Economics and Business Review*, vol. 4, núm. 1, 2020.

MARTIN, J. "Lost on the Silk Road: Online drug distribution and the 'cryptomarket'". *Criminology & Criminal Justice*, vol. 14, núm. 3, 2013.

MARTÍNEZ MARTÍNEZ, M. "Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago". *Revista de Pensamiento Estratégico y Seguridad CISDE*, núm. 1, 2016.

MARZHA, A.; ASSEM, U. & KI-JOUNE, L. "Detecting Hawala network for money laundering by graph mining". *The Journal of Finance and Data Science*, núm. 10, 2014.

MEDRANDA, N. & ARCOS, M. "Criptoactivos y criptomonedas". *Blockchain, criptoactivos y metaverso. Una aproximación teórica*. Editorial Abya-Yala, 2023.

MERAJ, M.; OZER, A. & KARABIYIK, U. "Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS". *Applied Sciences*, vol. 12, núm. 21, 2022.

MICCOLI, A. *Hawala and cryptocurrencies: a new avenue for terrorist financing* [Trabajo de Fin de Máster, Luiss Guido Carli]. Biblioteca LuissThesis, 2023.

MOHAMAD, A. & CHE HUSSIN, A. "Understanding Crowdfunding via Social Media: A Review of the Relevancy of Previous Studies". *International Journal of Academic Research in Business and Social Sciences*, vol. 14, núm. 1, 2024.

MOLINA, X.; MARTÍNEZ, L. & DEL CORTE, V. "Análisis del fenómeno del crowdfunding. El caso de la Plataforma Verkami". *Economía Industrial*, núm. 402, 2016.

MOVCHAN, A; SHLIAKHOVSKYI, O.; KOZIL, V. & FEDCHAK, I. "Investigating cryptocurrency financing crimes terrorism and armed aggression". *Social & Legal Studios*, vol. 6, núm. 4, 2023.

MALLADA, C. "La financiación del terrorismo desde la perspectiva de las nuevas tecnologías. A propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo". En *Anuario de Derecho Penal y Ciencias Penales*, vol. 71, 2018.

MALLADA, C. "Análisis de la gestión financiera y la estructura de las organizaciones terroristas. Los riesgos emergentes de financiación del terrorismo". *Anuario de Derecho Penal y Ciencias Penales*, fasc. 1, 2021.

MARTÍ, J. "La propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos: La propuesta MiCA". *Revista de Derecho del Sistema Financiero*, núm. 1, 2021.

MERINO HERRERA, J. "Estrategias de persecución penal contra la financiación del terrorismo". En *Revista Penal México*, núm. 8, 2015.

MIRABILE, M. "Debating Hawala, Infrastructures and Critical Issues: A Continuum from Hawala to Blockchain Technologies?". En *CONFINES*, año 18, núm. 34, 2022.

MIQUEL GÓNZALEZ, J. "Cláusulas generales y desarrollo judicial del Derecho". *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, núm. 1, 1997.

MOMBLANC, L. "Legalidad versus tipos penales abiertos en el Código Penal cubano". *Lex*, núm. 11, año 11, 2013.

MONTERO GUERRA, J. "Análisis psicológico del terrorismo". *Anuario de Psicología Jurídica*, vol. 7, núm. 1, 1997.

MONTES NOBLEJAS, D. "A vueltas con el terrorismo e Internet: Hacia una definición de ciberterrorismo". En *Revista de Derecho UNED*, núm. 27, 2021.

MOOIJ, A. *Regulating the Metaverse Economy. How to Prevent Money Laundering and the Financing of Terrorism*. Springer, 2023.

MORCILLO JIMÉNEZ, J. "Delitos contra el orden público". *Lecciones de Derecho Penal, Parte Especial*. Elena Marín de Espinosa (dir.). Editorial Tirant Lo Blanch, 4^a ed., 2023.

MORITZ, A. & BLOCK, J. "Crowdfunding: A Literature Review and Research Directions". *Crowdfunding in Europe. State of the Art in Theory and Practice*. FGF Studies in Small Business and Entrepreneurship, Springer. Dennis Brüntje y Oliver Gajda (edit.), 2016

MUÑOZ CONDE, F. *Derecho Penal, Parte Especial*. Editorial Tirant Lo Blanch, 23^a ed., 2021.

MUÑOZ CONDE, F. & GARCÍA ARÁN, M. *Derecho Penal. Parte General*, 8^a Edición. Tirant Lo Blanch, 2010.

NAVARRO CARDOSO, F. "Los tipos dolosos del delito de financiación del terrorismo". *Revista Electrónica de Ciencia Penal y Criminología*, núm. 20, 2018.

NÚÑEZ CASTAÑO, E. "El terrorismo en la era de la *globalización*: el delito de financiación del terrorismo ante el nuevo concepto de terrorismo". *Globalización y lucha contra las nuevas formas de criminalidad transnacional*, Alfonso Galán y Silvia Mendoza (coords.). Editorial Tirant Lo Blanch, 2019.

OGUZ, E.; BASAK, N. & KAPUSUZOGLU, A. "The use of crypto coins to finance terrorism". *Economic Science*, vol. 20, 2021.

OLMEDO CARDENETE, M. "Delitos contra el orden público (VI): De las organizaciones y grupos terroristas. Delitos de terrorismo". *Sistema de Derecho penal. Parte especial*. Lorenzo Morillas Cueva (dir.), 2024.

ORDÓÑEZ PONZ, F. "Investigación y cooperación judicial en los delitos en los que intervengan criptomonedas". *Cooperación judicial civil y penal en la Unión Europea. Retos pendientes y nuevos desafíos ante la transformación digital del proceso*, Paulo Suárez y Ana María Vicario (dirs.). Editorial Bosch Procesal, 2023.

OREHEK, E.; FISHMAN, S.; DECHESNE, M.; DOOSJE, B.; KRUGLANSKI, A.; COLE, A.; SADDLER, B. & JACKSON, T. "Need for Closure and the Social Response to Terrorism". *Basic and applied social psychology*, núm. 32, 2010.

PAREDES, J.M. "El 'terrorista' ante el Derecho penal: por una política criminal intercultural". En *Revista Nuevo Foro Penal*, vol. 6, núm. 74, 2010.

PASTRANA, S. & SUAREZ-TANGIL, G. "A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth". En *IMC '19: Proceedings of the Internet Measurement Conference*, 2019

PÉREZ CEPEDA, A. "Política criminal contra el terrorismo en la actualidad". *Perspectiva multidimensional del conflicto penal: de la política criminal a la concreción normativa "la línea invisible"*, Arnel Medina Cuenca (dir.). Unión Nacional de Juristas de Cuba, 2019.

PÉREZ MEDINA. "Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo". *Boletín Criminológico*. Edición especial, núm. 206, 2020.

PÉREZ ROYO, J. "La democracia frente al terrorismo global". *Terrorismo, democracia y seguridad, en perspectiva constitucional*. Editorial Marcial Pons, Javier Pérez Royo (dir.) y Manuel Carrasco Durán (coord.), 2010.

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

POVEDA, M. & TORRENTE, B. "Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista". *Opción*, año 32, núm. esp. 8, 2016.

PRADA GONZÁLEZ, J. "La onerosidad y gratuidad de los actos jurídicos". *Anales de la Academia Matritense del Notariado*, tomo 16, 1968.

RAHIMIAN, R. & CLARK, J. "TokenHook: Secure ERC-20 smart contract". *arXiv*, núm. 2107.02997, 2021.

RANSTORP, M. "La financiación del terrorismo: principales actores, estrategias y fuentes". *Afkar*, Tendencias Económicas, 2018.

RAZAVY, M. "Hawala: An underground haven for terrorists or social phenomenon?". *Crime, Law & Social Change*, núm. 44, 2005.

REIMER, S. & REDHEAD, M. "Bit by Bit Impacts of New Technologies on Terrorism Financing Risks". RUSI Europe y Project Craaft, 2022.

REY, P; RIVAS, P. & SÁNCHEZ, O. "Propaganda, radicalismo y terrorismo: la imagen del Daesh". *Estudios sobre el mensaje periodístico*, núm. 23, 2017.

REZAEINEJAD, I. "Challenges and opportunities cryptocurrency in Iran economy & e-businesses". *RUDN Journal of Economics*, vol. 29, núm. 4, 2021.

RODRÍGUEZ MORALES, T. "El terrorismo y nuevas formas de terrorismo". *Espacios Públicos*, vol. 15, núm. 33, 2012.

ROMANIUK, P. "The State of the Art on the Financing of Terrorism". *he RUSI Journal*, vol. 159, núm. 2, 2015.

ROSALINE, N. & NYAMWAYA, O. "The Dark Web and Cryptocurrencies: A 'trust' dilemma for digital commerce?". *Baraton Interdisciplinary Research Journal*, núm. 8, 2018.

ROSENFELD, R. "Terrorism and Counter-Terrorism: Criminological perspectives". *Sociology of Crime, Law and Deviance*, El Sevier, vol. 5, 2004.

ROXIN, C. *Teoría del Tipo Penal. Tipos Abiertos y Elementos del Deber Jurídico*. Traducido al español por Enrique Bacigalupo. Ediciones De palma, 1979.

RUPÉREZ, J. "Las Naciones Unidas en la Lucha contra el Terrorismo. Primer Balance". *Cuadernos de Pensamiento Político*, núm. 5, 2005.

RUSSO, ŠRNDIĆ y LASKOV. "Detection of illicit cryptomining using network metadata". *EURASIP Journal on Information Security*, núm. 1, 2021.

RYDER, N. "Terrorism financing and fraud – the unseen (seen) nexus?". *Countering Terrorism Financing*. Centre of Excellence Defence Against Terrorism, Nicholas Ryder (edit.), 2022.

RYUNG HAN, C. & NELEN H. "A living financial fossil, hawala: the evolution of informal fund transfer systems in Korea". *Trends in Organized Crime*, vol. 28, núm. 1, 2025.

SALDAÑA TABOADA, P. "Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes". [Tesis de doctorado no publicada]. Universidad de Granada, 2023.

SANTANDREU, F. "Criptomonedas: ¿regular o no regular en el nivel español y europea? He ahí la cuestión". *Revista Universitaria Europea*, núm. 39, 2023

SÁNCHEZ MEDERO, G. "Las fuentes de financiación legales e ilegales de los grupos terroristas". *Revista Política y Estrategia*, núm. 112, 2008.

SCHMEELK, S.; ROSADO, B. & BLACK, P. "Blockchain Smart Contracts Static Analysis for Software Assurance". *Intelligent Computing Proceedings of the 2021 Computing Conference, Volume 2*, Springer, vol. 284, 2021.

SCHMID, A. "Frameworks for conceptualising terrorism". *Terrorism and Political Violence*, vol. 16, núm. 2, 2004.

SILALAHI, J.; BUHARA, T.. & HENDRATNO, S. "Young Generation Point of View About Non-Fungible Token as a Future Currency and Assets". *E3S Web of Conferences*, núm. 426.

SOOD, K.; SINGH, S.; BEHL, A.; SINDHWANI, R.; KAUR, S. & PEREIRA, V. "Identification and prioritization of the risks in the mass adoption of artificial intelligence-driven stable coins: The quest for optimal resource utilization". *Resources Policy*, vol. 81, 2023.

SUÁREZ DE LEZO. "Principales implicaciones del Reglamento MiCA para las entidades del mercado de criptoactivos". *CMS Albiñana*, 2023.

TAMARIT SUMALLA, J. "Ciberterrorismo. Regulación y estrategias para combatirlo". Universitat Oberta de Catalunya, 2020.

TERRADILLOS, J. "El Estado de Derecho y el fenómeno del terrorismo". *Terrorismo y Estado de Derecho*. Editorial Iustel, José Ramón Serrano y Eduardo Demetrio (dirs.), 2010.

TOMPKINS, P. & BOS, N. *Human factors considerations of undergrounds in insurgencies*. Fort Bragg, North Carolina, United States Army Special Operations Command. 2da Edición, 2013.

TORRES FERNÁNDEZ, M. "La regulación de la responsabilidad penal de las personas jurídicas por delitos de terrorismo. El terrorismo, ¿riesgo en el tráfico jurídico y empresarial?". *Anuario de Derecho Penal y Ciencias Penales*, tomo 73, fasc. 1, 2020.

TORRES VÁSQUEZ, H. "El concepto de terrorismo, su inexistencia o inoperancia: La apertura a la violación de derechos humanos". En *Diálogos de Saberes*, núm. 32, 2010.

TRAUTMAN, L. "Virtual currencies; Bitcoin & What now after Liberty Reserve, Silk Road, and Mt. Gox?". *Richmond Journal of Law & Technology*, vol. 20, núm. 4, 2014.

VALERI, M.; FONDACARO, R.; DE ANGELIS, C. & BARELLA, A. "The Use of Cryptocurrencies for Hawala in the Islamic Finance". *European Journal of Islamic Finance*, núm. esp. EJIF Workshop, 2020.

WANG, S. & ZHU, X. "Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing". *Policing: A Journal of Policy and Practice*, vol. 15, núm. 4, 2021.

WEIMANN, G. "Terrorismo e Internet". *Etic@ net*, núm. 3, 2010.

ZARAGOZA AGUADO, J. "Artículo 576". *Comentarios Prácticos al Código Penal*, tomo VI. Manuel Gómez (dir.), Aranzadi, 2015.

ZUNZUNEGUI, F. "Encuadre sistemático y conceptual de la financiación participativa (Crowdfunding)". *Aspectos legales de la financiación en masa o crowdfunding*. Editorial Tirant Lo Blanch. Matilde Cuena (dir), 2020.

Otras fuentes

BLANCO CORDERO. "La modalidad imprudente del delito de blanqueo de capitales". *VI Jornadas sobre prevención y represión del blanqueo de capitales*. Abogacía Española, 2018. <https://www.abogacia.es/wp-content/uploads/2018/12/3delitoblanqueo.pdf>

BOZKURT, A. "U.S. Crackdown on Hamas Virtual Currency Sheds Light on Turkey's Role in Terrorism Financing". Middle East Forum, 3 de abril de 2025. <https://www.meforum.org/mef-online/u-s-crackdown-on-hamas-virtual-currency-sheds-light-on-turkeys-role-in-terrorism-financing>

CHAINALYSIS. "Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns", 8 de julio de 2021.

COMISIÓN EUROPEA. "Desmitificando los Tokens No Fungibles o NFT". *Diario La Ley*, 2021. <https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbH1czUwMDAyDA-2MzZUK0stKs7Mz7M1AooYGhkagAQy0ypd8pNDKgtSbdMSc4pTAa-JefJw1AAAWKE>

COUNTER EXTREMISM PROJECT. "Far-Right European Terrorist Group Crowdfunding Cryptocurrency" [Nota de Prensa], agosto de 2018. <https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency>

COUNTER EXTREMISM PROJECT. "Extremist Content Online: Pro-ISIS Online Chat Promotes Monero Cryptocurrency To Fund Propaganda Operations" [Nota de Prensa], junio de 2023. <https://www.counterextremism.com/press/extremist-content-online-pro-isis-online-chat-promotes-monero-cryptocurrency-fund-propaganda>

CYBER THREAT ALLIANCE. "The illicit cryptocurrency mining threat". Informe, 2018. <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf>

DEPARTAMENTO DEL TESORO DE LOS ESTADOS UNIDOS. "United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers" [Comunicado de Prensa], 14 de noviembre de 2023. <https://home.treasury.gov/news/press-releases/jy1907>

DEPARTAMENTO DE SEGURIDAD NACIONAL DE LOS ESTADOS UNIDOS. “Combatting illicit activity utilizing financial technologies and cryptocurrencies”. Public-Private Analytic Exchange Program, 2022.

DEPARTAMENTO DE SEGURIDAD NACIONAL DE LOS ESTADOS UNIDOS. “Ransomware Attacks on Critical Infrastructure Sectors”. Public-Private Analytic Exchange Program, 2022.

ELLIPTIC. “How terrorist groups are exploiting crypto to raise funds and evade detection”. Reporte, 17 de Agosto de 2023. <https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-e evade-detection>

ESMA. Advice Investment-based crowdfunding, 2014. https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1560_advice_on_investment-based_crowdfunding.pdf

EUROPEAN BANKING AUTHORITY. Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. EBA/GL/2024/11, 4 de julio de 2024.

FINANCIAL INTELLIGENCE CENTRE. Assessment of the Money Laundering and Terrorist Financing Risk. Crypto Asset Service Providers, 1 de abril de 2025.

FROST. “Terroristas usaron cupones de criptomonedas para enviar dinero de Francia a Siria” [Comunicado de prensa]. Decrypt, 30 de septiembre de 2020. <https://decrypt.co/es/43402/terroristas-usaron-cupones-de-criptomonedas-para-enviar-dinero-de-francia-a-siria>

GAFI. IX Special Recommendations. Revisión de 2012. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf>

GAFI. “The role of hawala and other similar service providers in money laundering and terrorist financing”. Reporte, 2013.

GAFI. “Crowdfunding for terrorism financing”. Informe, 2023. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf>

GAFI. Lavado de dinero y financiamiento del terrorismo en el mercado del arte y las antigüedades. Reporte, 2023. <https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/reports/Spanish-ML-TF-Art-Antiquities-Market.pdf.coredownload.pdf>

GOBIERNO DE ESPAÑA. Estrategia Nacional contra el Terrorismo, 2019.

HUILLET. “La policía francesa arresta a una red de financiación del terrorismo que usaba cupones de Bitcoin” [Comunicado de prensa]. Cointelegraph, 30 de septiembre de 2020. <https://es.cointelegraph.com/news/french-police-arrest-terror-financing-ring-that-used-bitcoin-coupons>

HUMPHRY, R.; AVRAMOVIC, P.; ACEVEDO, F.; ALKHAIR, S. & GERVAIS, A. Review of Maximal Extractable Value & Blockchain Oracles. Research Note, FCA, 2024

KATTE, S. "Los grupos terroristas podrían recurrir a los NFT para recaudar fondos y difundir mensajes" [Artículo de prensa]. Cointelegraph, 05 de septiembre de 2022. <https://es.cointelegraph.com/news/terror-groups-may-turn-to-nfts-to-raise-funds-and-spread-messages-wsj>

MEMRI. "A Review Of Al-Sadaqah Organization's Activity On Telegram: Group Updates Its WhatsApp Number, Uses Deep Web-Based Email Service SecMail" [Nota de Prensa], agosto de 2018. <https://www.memri.org/cjlab/a-review-of-al-sadaqah-organizations-activity-on-%C3%A2%E2%82%AC%C5%BEtelegram-group-updates-its-whatsapp-number-uses-%C3%A2%E2%82%AC%C5%BEdeep-web-based-email-service-secmail>

MEMRI. "Pro-Al-Qaeda Telegram Bot Solicits Cryptocurrency Donations For 'Operational Cell' In Gaza" [Nota de Prensa], octubre de 2023. <https://www.memri.org/cjlab/pro-al-qaeda-telegram-bot-solicits-cryptocurrency-donations-operational-cell-gaza>

MOORE, G. "Custody. Crypto Assets' Unique Challenge and Opportunity". Coindesk, 2019.

NACIONES UNIDAS. Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo. Informe del Secretario General, 2006.

NACIONES UNIDAS. Carta de fecha 11 de marzo de 2020 dirigida al Secretario General por el Representante Permanente de la Federación de Rusia ante las Naciones Unidas. Documento con referencia A/74/751-S/2020/204, preparado por la Reunión de Jefes de Servicios Especiales, Organismos de Seguridad y Órganos Encargados del Cumplimiento de la Ley, asumido como documento de la Asamblea General y del Consejo de Seguridad de las Naciones Unidas, 2020.

NORDIC MONITOR. "US Crackdown on Hamas virtual currency reveals Turkey's role in terrorism financing". FinCrime Central, s/f. <https://fincrimecentral.com/us-crackdown-hamas-crypto-turkey-financing/>

ONDACERO. "Territorio Negro: Los camaleones de la Policía y los falsos vacunados de Covid" [Comunicado de Prensa], 31 de mayo de 2022. https://www.ondacero.es/programas/julia-en-la-onda/audios-podcast/territorios/negro/territorio-negro-camaleones-policia-falsos-vacunados-covid_202205316296346ed7b96e0001f87560.html

OFICINA DE LUCHA CONTRA EL TERRORISMO. "Lucha contra la financiación del terrorismo". Naciones Unidas, s/f. <https://www.un.org/counterterrorism/es/cct/countering-the-financing-of-terrorism>

O'LEARY, R. "The bitcoin terrorists of Idlib are learning new tricks" [Artículo de Prensa]. WIRED, 2021. <https://www.wired.com/story/bitcoin-crypto-terrorism-syria/>

ORGANIZACIÓN DE ESTADOS AMERICANOS. *Guía Práctica de Prevención, Detección y Represión del Financiamiento del Terrorismo*, 2007.

PACCHIANI, G. "Terrorists raised \$130m in crypto since 2021; sought more via social media after attack" [Artículo de Prensa]. The times of Israel, octubre de 2023. <https://www.timesofisrael.com/gazan-terror-groups-raised-over-130-million-in-crypto-to-fund-attack/>

PLADSON, K. "Cómo las criptomonedas facilitaron el ataque de Hamás" [Artículo de Prensa]. DW, 16 de octubre de 2023. <https://www.dw.com/es/c%C3%B3mo-las-criptomonedas-facilitaron-el-ataque-terrorista-de-ham%C3%A1s-contra-israel/a-67114348>

REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española* (23^a Edición), 2014.

ROMANOV, Y. & TUKAEVA, A. "Minería ilegal de criptomonedas: impacto en el comercio y la regulación" [Artículo de prensa]. Crypto Robotics, 10 de enero de 2025. <https://cryptorobotics.ai/es/news/illegal-crypto-mining-impact-trading-regulation/>

SENAZO ESPAÑOL. Respuesta del Gobierno a las preguntas 684/62456 y 684/62534, 684/64319 y 684/64414 y 684/64424. Secretaría de Estado de Relaciones con las Cortes y Asuntos Constitucionales, 2023.

TALLEY, I. "Islamic State Turns to NFTs to Spread Terror Message" [Comunicado de Prensa]. The Wall Street Journal, 6 de septiembre de 2022. <https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800>

TERRADILLOS. "La red de pasaportes COVID falsos cobraba en criptomonedas desde cuentas abiertas en el Campo de Gibraltar y Lituania" [Comunicado de Prensa]. Cadena Ser, 28 de enero de 2022. <https://cadenaesr.com/2022/01/28/la-red-de-pasaportes-covid-falsos-cobraba-en-criptomonedas-desde-cuentas-abiertas-en-el-campo-de-gibraltar-y-lituania/>

THE COINOMIST. "Terrorist groups are actively using stablecoins" [Artículo de prensa], 16 de octubre de 2023. <https://coinomist.com/breaking-news/terrorist-groups-are-actively-using-stablecoins/>

THE HINDU. "Trading in Bitcoin in India is refined way of doing Hawala business: Supreme Court" [Nota de prensa]. PTI, 6 de mayo de 2025. <https://www.thehindu.com/news/national/trading-in-bitcoin-in-india-is-refined-way-of-doing-hawala-business-supreme-court/article69543528.ece>

THE NATION. "Illegal crypto mining machines seized from abandoned houses" [Comunicado de prensa], 15 de marzo de 2025. <https://www.nationthailand.com/news/general/40047447>

TRADE REPUBLIC. Información sobre el riesgo de las operaciones con criptomonedas, 2024. <https://assets.traderepublic.com/assets/files/Crypto%20ES%20%20Disclaimer%20Document.pdf>

TRM. *Crypto Crime Report*, 2025.

UNODC. "The Hawala System. Its operations and misuse by opiate traffickers and migrant smugglers". Afghan Opiate Trade Project y UNODC Research, 2023.

VEDRENNE. "Cupones' de Criptomonedas Financiaron el Yihadismo Sirio, Afirman Autoridades Francesas" [Comunicado de prensa]. Acams Conexión, 13 de octubre de 2020. <https://www.acamstoday.org/cupones-de-criptomoneda-financiaron-el-yihadismo-sirio-afirman-autoridades-francesas/>

WARRETH, S. "Crowdfunding and Cryptocurrency Use by Far-Right and Jihadi Groups" [Artículo de Prensa]. Vox Pol, 2019 (actualizado en 2024). <https://voxpol.eu/crowdfunding-and-cryptocurrency-use-by-far-right-and-jihadi-groups/>.

WILLIAMSON, M. "Israeli Authorities Seize 30 Crypto Wallets Linked to Financing Terrorism". Finance Magnates, 28 de febrero de 2022. <https://www.financemagnates.com/cryptocurrency/israeli-authorities-seize-30-crypto-wallets-linked-to-financing-terrorism/>.

Referencias legislativas

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 281, de 24 de noviembre de 1995. <https://www.boe.es/eli/es/lo/1995/11/23/10/con>

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. *Boletín Oficial del Estado*, 45, de 21 de febrero de 2019. <https://www.boe.es/eli/es/lo/2019/02/20/1>

Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas, y por el que se modifican el Reglamento (UE) 2017/1129 y la Directiva (UE) 2019/1937. *Diario Oficial de la Unión Europea*, 347, de 20 de octubre de 2020. Referencia: DOUE-L-2020-81532

Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo de 31 de mayo de 2023 relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849. *Diario Oficial de la Unión Europea*, 150, de 9 de junio de 2023. Referencia: DOUE-L-2023-80807.

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937. *Diario Oficial de la Unión Europea*, 150, de 9 de junio de 2023. Referencia: DOUE-L-2023-80808

Referencias jurisprudenciales

TRIBUNAL SUPREMO (Sala de lo Penal, Sección 2^a), Nº de Resolución: 540/2010, Nº de Recurso: 2521/2009, de 08 de junio de 2010. ECLI:ES:TS:2010:2903.

TRIBUNAL SUPREMO (Sala de lo Penal, Sección 1^a), Nº de Resolución: 439/2014, Nº de Recurso: 2261/2013, de 10 de julio de 2014. ECLI:ES:TS:2014:2815.

TRIBUNAL SUPREMO (Sala de lo Penal, Sección 1^a), Nº de Resolución: 326/2019, Nº de Recurso: 998/2018, de 20 de junio de 2019. ECLI:ES:TS:2019:2109.

TRIBUNAL SUPREMO (Sala de lo Penal, Sección 1^a), Nº de Resolución: 20770/2024, Nº de Recurso: 20038/2024, de 02 de julio de 2024. ECLI:ES:TS:2024:8765A.

AUDIENCIA NACIONAL (Sala de lo Penal N.º 2) N.º de Resolución: 21/2023, N.º de Recurso: 6/2022, de 3 de octubre de 2023. ECLI: ES:AN:2023:4682.

AUDIENCIA NACIONAL (Sala de lo Penal, Sección Apelación), Nº de Resolución: 1/2024, Nº de Recurso: 23/2023, de 9 de enero de 2024. ECLI: ES:AN:2024:53.

