



SABER, arte y técnica

Minerva. Saber, arte y técnica

AÑO VII • VOL. 1 • JUNIO - DICIEMBRE 2023

ISSN en línea 2545-6245

ISSN impreso 2591-3840

Financiamiento DEL TERRORISMO 2.0: el uso de criptoactivos para financiar operaciones terroristas

MANUEL SANTOS MAILLAND*
Universidad Austral (UA).
Universidad del Museo Social
Argentino (UMSA), Argentina
manusantosmai@gmail.com

RECIBIDO: 31 de marzo de 2023
ACEPTADO: 4 de mayo de 2023

Resumen El presente artículo indaga en una temática de interés global: el financiamiento del terrorismo con la particularidad de la utilización de criptoactivos. Para trabajar dicha problemática se analiza la figura delictual del art. 306 del Código Penal argentino. Además, se realiza un breve repaso sobre las especificidades de la tecnología de criptoactivos, para luego abordar, desde una perspectiva práctica, dos casos reales de financiamiento del terrorismo a través del uso de dichas tecnologías.

Palabras clave criptoactivos; criptomonedas; financiamiento del terrorismo (FT); terrorismo; trazabilidad; investigaciones criminales

Financing of Terrorism 2.0: the Use of Crypto-Assets to Finance Terrorist Operations

Abstract This article develops a globally relevant topic: terrorism financing, with a particular focus on the use of crypto-assets. To address this issue, the offense provided for in Section 306 of the Argentine Criminal Code is to be analyzed. Said section also provides a brief overview of the particularities

of crypto-asset technology, before analyzing two real-life cases of terrorism financing through the use of these technologies from a practical perspective.

Keywords crypto-assets; cryptocurrencies; finance of terrorism (FT); terrorism; trazability; criminal investigations

Introducción El terrorismo es sin dudas un estigma global. No hace falta ejemplificar los flagelos que ha producido a la humanidad para comprenderlo mejor. Argentina no ha quedado al margen de dicha problemática, ha sufrido en su historia reciente actos concretos de terrorismo –como los atentados a la Embajada de Israel y a la sede de la AMIA–, cuyas repercusiones sociales en varias dimensiones se hacen presentes hasta hoy en día.

La globalidad en la que vivimos no ha hecho más que acrecentar el poder operativo que grupos de distintas partes del mundo tienen para infligir aun más daño. La existencia de células dormidas o “llaneros solitarios” son algunos ejemplos del nuevo *modus operandi* de estos grupos, donde con tan solo un mensaje a través de alguna plataforma de mensajería instantánea se pueden activar hechos de una atrocidad indescriptible.

Dejando de lado este aspecto, un subproducto de los hechos de terrorismo, de vital importancia para la ejecución de estos, es la temática relativa a su financiamiento. Buscando atacar la raíz misma de este mal, los estados y organizaciones internacionales han llegado a comprender que la pregunta por el financiamiento es el modo más eficaz para comenzar a dismantelar este tipo de problemática social. Desde este nuevo enfoque, se explica que la banca tradicional se encuentre sujeta a rigurosos controles respecto de sus clientes y sus respectivas operaciones diarias, con el fin de evitar el arribo de fondos a manos terroristas.

La Argentina no es ajena a esta nueva perspectiva de control financiero, debido mayormente a sus compromisos internacionales derivados de su participación en el mercado global. Aunque, en un primer momento, puede parecer que nuestro país es ajeno a esta clase de hechos de financiamiento del terrorismo, el caso del “Clan Barakat” (Nabot, 2018), en la provincia de Misiones –en la zona denominada Triple Frontera– demuestra que, en efecto, sí se han cometido hechos de este tipo en nuestra jurisdicción –y probablemente vuelvan a ocurrir, pues ningún sistema de prevención es infalible–.

Como era de esperarse, los criminales y, en este caso concreto, los financistas de esta clase de operaciones, siempre se encuentran primeros en la carrera por la innovación en el despliegue de nuevas tecnologías para facilitar su conducta delictual. La digitalización de la economía hace que las clásicas fronteras entre los estados se desdibujen y no requiera tanto esfuerzo burlar los controles financieros, sumado al hecho de que los sujetos podrían encontrarse a miles de kilómetros de distancia.

En los últimos años, una de las tecnologías utilizadas en el financiamiento del terrorismo fue la de los *criptoactivos* (Faucon *et al.*, 2021). Algunas de las particularidades que poseen este tipo de activos han hecho de él una herramienta sumamente útil tanto para los financistas del terrorismo como para los mismos terroristas. No es difícil imaginar que, en este contexto tecnológico, resulta de mayor sencillez el envío de un Bitcoin que dólares en un sobre. Sin embargo, son

estas mismas particularidades, las que permiten —y ya permitieron— rastrear los fondos de una manera relativamente sencilla, pero sobre todo efectiva, terminando así con el flujo de dinero que solventa las operaciones de terrorismo.

A continuación, se presentará cómo la utilización de criptoactivos en criminalidad compleja, y específicamente en lo relativo al financiamiento del terrorismo, ha brindado los medios tecnológicos para que puedan desarrollarse dichas actividades, aunque sin duda alguna dicha tecnología no ha sido la panacea para los criminales (Chainalysis, 2020).

Antes de avanzar en el análisis del uso de criptoactivos en operaciones de financiamiento del terrorismo, es importante entender cómo funciona este tipo penal. Para ello, nos valdremos de la tipificación que se hace del delito en Argentina, y aunque los casos que veremos no se llevarán a cabo en nuestra jurisdicción, servirán para ilustrar el fenómeno.

Financiamiento del terrorismo en Argentina

La denominada “Ley Antiterrorista” responde a un momento particular socio-histórico. Luego de los atentados a las torres gemelas en los Estados Unidos, y con el fin de atacar el motor financiero de este tipo de ataques terroristas, el foco pasó al financiamiento económico de aquellos grupos extremos, entre otros instrumentos internacionales que marcan esta postura, a la cual suscribe nuestro país. Aboso realiza una recopilación de la normativa sobre dichas temáticas, menciona la Resolución 1373 del Consejo de Seguridad de la ONU,¹ el Convenio Internacional para la Represión de la Financiación del Terrorismo, la Convención Interamericana contra el Terrorismo y las recomendaciones de GAFI (Aboso, 2019; Pieralisi *et al.*, 2018).

Por otro lado, la UNODC,² la oficina especializada en criminalidad transnacional de la ONU, lo define como el proceso que “abarca los medios y métodos utilizados por las organizaciones terroristas para financiar actividades que representan una amenaza para la seguridad nacional e internacional” (UNODC, s.f.). Esos medios, añade, pueden provenir de un origen tanto lícito como ilícito y, a diferencia del lavado de activos, este proceso es lineal, en cuanto a que los fondos generados para financiar estas actividades no vuelven a dicho originante, sino que son utilizados por el terrorista o grupo terrorista para financiar sus actividades.

Así, respetando la tendencia internacional, en diciembre de 2011, se incorpora al Código Penal argentino, a través de la Ley 26.734, el artículo 306. Este tipifica el delito de “financiamiento del terrorismo” y, tal como lo indica, penaliza a quien sea que ayude económicamente a la comisión de actos de terrorismo. A continuación, el mencionado artículo, tal como surge de su redacción en el Código Penal.

Art. 306

1. Será reprimido con prisión de cinco (5) a quince (15) años y multa de dos (2) a diez (10) veces del monto de la operación, *el que directa o indirectamente recolectare o proveyere bienes o dinero, con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte:*

a) Para financiar la comisión de un delito con la finalidad establecida en el artículo 41 quinquies;

1. https://www.unodc.org/pdf/crime/terrorism/res_1373_spanish.pdf

2. Oficina de Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés).

b) Por una organización que cometa o intente cometer delitos con la finalidad establecida en el artículo 41 quinquies;

c) Por un individuo que cometa, intente cometer o participe de cualquier modo en la comisión de delitos con la finalidad establecida en el artículo 41 quinquies.

2. Las penas establecidas se aplicarán independientemente del acaecimiento del delito al que se destinara el financiamiento y, si éste se cometiere, aún si los bienes o el dinero no fueran utilizados para su comisión.

3. Si la escala penal prevista para el delito que se financia o pretende financiar fuera menor que la establecida en este artículo, se aplicará al caso la escala penal del delito que se trate.

4. Las disposiciones de este artículo regirán aun cuando el ilícito penal que se pretende financiar tuviere lugar fuera del ámbito de aplicación espacial de este Código, o cuando en el caso del inciso b) y c) la organización o el individuo se encontraran fuera del territorio nacional, en tanto el hecho también hubiera estado sancionado con pena en la jurisdicción competente para su juzgamiento.

De aquí se extrae que se tipifica el accionar de quien financie –recolectando o proveyendo–, directa o indirectamente, con dinero o bienes, sabiendo o debiendo saber, un hecho del artículo 41 quinquies, llevado a cabo por una organización o un individuo.

Continuando con la exégesis de dicho artículo 306, y en cuanto a sujeto activo, vemos que es un delito común, es decir, no se requiere que quien financia sea un sujeto activo especial, puede ser cualquier individuo. Esta persona debe “recolectar” o “proveer”, para configurar el tipo penal. De acuerdo con la Real Academia Española, el primero de estos verbos, en su segunda acepción,³ significa “Reunir cosas o personas de procedencia diversa”, mientras que el segundo brinda dos opciones igualmente válidas: “Preparar, reunir lo necesario para un fin” y “Suministrar o facilitar lo necesario o conveniente para un fin”.⁴ Estas definiciones parecen demostrar una cierta redundancia en la utilización de dos verbos típicos, que pueden expresar el mismo tipo de accionar, sobre todo cuando vienen precedidos por los vocablos “directa” o “indirectamente”. El hecho de que estén ambos presentes, en definitiva, no es contraproducente, sino magra técnica legislativa, especialmente cuando hay que analizar el rol de entidades bancarias o financieras que intermedian neutralmente –o no– en operaciones diarias que puedan estar financiando actos terroristas.

A su vez, esos verbos típicos deben ser enfocados hacia dos tipos de activos, “bienes” o “dinero”. En el primer caso, de acuerdo con Blanco Cordero (2015), se trata de “cualquier activo que tenga valoración económica”. Así, con la utilización de este vocablo, no habría necesidad de incorporar la palabra “dinero”, pues su definición engloba ambos activos (Merger, 1892).

En cuanto al *quién* es financiado, el artículo provee de tres opciones. La primera de ellas será para quien financie a quien, a su vez, está financiando un acto terrorista. La finalidad es evitar la atipicidad que se podría generar al intentar *estratificar* la operación entre varios individuos. Las otras dos opciones que ofrece este artículo se refieren a la comisión de hechos de modo individual o grupal, es decir, quien financie a una persona individual o a un grupo para la comisión de un acto terrorista.

3. <https://dle.rae.es/recolectar?m=form>

4. <https://dle.rae.es/proveer?m=form>

Para completar la figura, el artículo reenvía al artículo 41 quinquies,⁵ que es el que define actos de terrorismo, es decir que cualquiera de estas tres hipótesis debe ir acompañada de la finalidad este artículo.

Todo lo anterior nos lleva a decir que es un *delito de peligro abstracto y autónomo*, pues en su punto dos aclara que no se requiere la consecución de un acto de terrorismo para que se encuentre realizado el tipo penal.

A su vez, en el punto cuatro, se le da una impronta *extraterritorial* a la figura, reforzando su autonomía mencionada anteriormente, pues no es necesario que el individuo o grupo al que se trata de financiar se encuentre en nuestro país. En el mismo punto, sin embargo, exige que los hechos de los incisos b) y c) también se encuentren sancionados en aquel país.

A continuación se tratará qué son los criptoactivos, previo a entender cómo pueden ser utilizados en maniobras que puedan o no encuadrar en esta figura típica.

Breve reseña de los criptoactivos y sus características

Los criptoactivos son la última tendencia en materia financiera y bancaria. Nacidos a fines de 2008, Bitcoin es el primero de su clase, creado por Satoshi Nakamoto, de quien actualmente se desconoce su verdadera identidad o identidades, pues muchos creen que podría tratarse de un grupo de desarrolladores, algunos de los cuales podrían haber formado parte del denominado grupo hacker Cyberpunks⁶ (Adams y Curry, 2023).

En cualquier caso, esta criptomoneda fue la primera de su clase, ideada para reemplazar a la plaza tradicional bancaria y todas sus características negativas, que fueron puestas de manifiesto en la crisis de las hipotecas *subprime* a nivel mundial.

5. Código Penal Argentino, Art. 41 quinquies: "Cuando alguno de los delitos previstos en este Código hubiere sido cometido con la *finalidad de aterrorizar a la población u obligar a las autoridades públicas nacionales o gobiernos extranjeros o agentes de una organización internacional a realizar un acto o abstenerse de hacerlo*, la escala se incrementará en el doble del mínimo y el máximo. Las agravantes previstas en este artículo no se aplicarán cuando el o los hechos de que se traten tuvieren lugar en ocasión del ejercicio de derechos humanos y/o sociales o de cualquier otro derecho constitucional". <http://servicios.infoleg.gob.ar/infolegInternet/anexos/190000-194999/192137/norma.htm>

6. Para profundizar en la historia de este grupo anarquista, se recomienda Nakamoto (30 de diciembre de 2019). The Cypherpunks. <https://nakamoto.com/the-cypherpunks/>.

Tal como dice Ramlall (2015),

la crisis subprime de los Estados Unidos, que empezó en 2007 con las grandes pérdidas manifestadas en el fondo de cobertura Bear Stearns, dejó atrás cicatrices permanentes en el sistema financiero. De todas las crisis financieras que han sacudido al planeta, la crisis subprime de los Estados Unidos es considerada única. (2)

Es en este contexto socio-histórico que, aprovechando desarrollos de software de las décadas precedentes más algunas innovaciones propias de Nakamoto, se creó un *sistema de pagos* descentralizado, transparente, pseudoanónimo y global. Siendo estas las características que la distinguen de los medios de pagos tradicionales de las sociedades actuales (Silva *et al.*, 2022). Analicemos brevemente estas condiciones:

- Descentralización: los criptoactivos no están controlados por ninguna autoridad central, sino que funcionan en una red descentralizada de usuarios, dándole independencia de cualquiera que quiera ejercer un rol preponderante.
- Pseudoanonimato: aunque no todos los criptoactivos son completamente anónimos, muchos de ellos ofrecen un alto nivel de privacidad y anonimato en las transacciones. Si se identifica la persona física utilizando una clave pública, dejará de ser anónima y se podrá trazar todo su historial de transacciones.

- Seguridad: la tecnología de criptografía utilizada en los criptoactivos asegura que las transacciones sean seguras y que los fondos no puedan ser robados o falsificados.
- Transparencia: todas las transacciones en una red de criptoactivos son públicas y se pueden ver en tiempo real en un registro llamado *blockchain*. En este mismo punto, y gracias a esta característica, hablamos de inmutabilidad, ya que una vez que una transacción se registra en la *blockchain*, no se puede revertir ni modificar.

Todas estas características han generado un halo de seguridad y confianza en Bitcoin, dándole la posibilidad a los usuarios de todo el mundo de contar con un sistema de pagos libre, rápido y global. Si bien es una tecnología que se encuentra en sus albores, ha probado ser disruptiva en muchos más aspectos que solo aquellos que hacen a las finanzas y al sistema bancario.

Así como con cualquier otro activo financiero y bancario en el que se pueda pensar, Bitcoin cuenta también con características negativas asociadas: I) La volatilidad de su cotización es noticia diaria en los portales de noticias de todo el mundo y II) una debatible fama asociada a la criminalidad compleja. Son solo dos ejemplos de las características negativas más destacadas.

Por otro lado, apropiadamente se habla de criptoactivo y no de criptomoneda, por una relación de género-especie. En ese sentido, Bitcoin no es el único de su clase, sino que ha sembrado las bases para otros tipos de activos. Desde el desarrollo de Ethereum en 2013 al día de la fecha, han surgido miles de criptoactivos de todo tipo y variedad, algunos novedosos, otros no tanto, pero todos aprovechan las bondades de que toda esta tecnología sea *open-source* (de código abierto).

Así, existen muchas categorizaciones, pero aquella que nos parece más pedagógica y apropiada para un mejor entendimiento de este menú de activos, es la adoptada por la FINMA (2018), la Autoridad de Supervisión de Mercados Financieros de Suiza. Esta ha establecido una clasificación para los criptoactivos que se basa en su función y en cómo se regulan en virtud de la legislación suiza (bajo la normativa “MiCA” de la Unión Europea –en inglés, *Markets in Crypto Assets Regulation*– se contará con otra triple categorización de este tipo de activos, aunque todavía no se encuentra en vigencia). Esta clasificación se divide en tres categorías:

- De pago (*payment token*): son criptoactivos que se utilizan principalmente como medio de pago o transferencia de valor.
- De utilidad (*utility token*): son criptoactivos que se utilizan para acceder a servicios o productos específicos dentro de una plataforma.
- De inversión (*asset or security token*): son criptoactivos que se utilizan para inversión, y que se comportan de manera similar a los valores tradicionales, como las acciones o los bonos.

En síntesis, podemos decir que Bitcoin es un sistema de pagos con características únicas, que ha generado un desarrollo de otro tipo de criptoactivos, de todas las variedades imaginables (Zocaro, 2022). Son herramientas financieras que tienden a la desintermediación y la eliminación del tercero de confianza, así como a facilitar la inclusión financiera y globalización. Estas características, así como el hecho de que gracias a ser completamente digital no reconoce fronteras, han despertado el interés de otros actores: los criminales.

La utilización de criptoactivos en operaciones de financiamiento del terrorismo

Previo a desarrollar los conceptos mencionados anteriormente a la vista de dos casos reales, se debe hacer un énfasis en cómo esta herramienta facilita el envío de fondos entre particulares. En el caso práctico que una persona residente en un país desee enviarle fondos a otra en un segundo país, deberá normalmente recurrir a una remesadora de fondos o realizar una transferencia internacional por intermedio de su banco y el banco receptor (usando la red SWIFT). Ambos procesos tienen la característica central de ser costosos y lentos.

Lo contrario ocurre al utilizar Bitcoin, o cualquier otro criptoactivo, lo cual facilita este tipo de operatoria drásticamente. En este caso, la persona que desee enviar los fondos comprará en alguna plataforma *exchange* el criptoactivo que desee. Luego, pedirá la clave pública asociada a la otra persona, sin importar el lugar de su residencia. Y al cabo de unos minutos, la otra persona tendrá en su poder los criptoactivos enviados, los cuales podrá conservar o acceder a bienes o servicios que acepten este medio o, por supuesto, liquidar los activos en la divisa de su país. Es esta última opción la más realizada, pues la adopción de los criptoactivos para transacciones es todavía muy baja a nivel mundial (Maldonado, 2020). Este sería, en síntesis, el recorrido para el envío de estos activos, mismo camino que utilizarán los criminales que deseen usar esta herramienta para, en última instancia, hacerse de dinero en efectivo.

En el caso argentino, vemos que el uso de criptoactivos es fácilmente subsumible en la figura del art. 306 y, por tanto, es posible financiar actos o grupos terroristas con estos activos. Estos, tal como dice Eraso Lomaquiz, “son, en cuanto a su naturaleza jurídica, bienes [...] los bitcoins, así como el resto de las monedas virtuales, son representaciones digitales de valor que, como tales, son intangibles” (2015). Tal como afirma Teichmann, “las criptomonedas son en efecto adecuadas para financiar el terrorismo” (2018).

En cuanto al rol de las mencionadas *exchanges* en operaciones de este tipo, sobre todo teniendo en cuenta la forma en la que se encuentra tipificado el financiamiento del terrorismo en nuestro código, es un tema que amerita un trabajo específico, aunque se puede adelantar que dependerá de las circunstancias del caso. La cuestión jurídica se centra en determinar si es o no una actividad neutra.

A continuación, se desarrollarán dos casos prácticos en los que se puede apreciar cómo distintos grupos terroristas han aprovechado los criptoactivos para financiar sus operaciones delictivas.

A. BRIGADAS AL-QASSAM

Hamas, que es un grupo señalado como organización terrorista por los Estados Unidos y la Unión Europea, gobierna en la Franja de Gaza desde el año 2007. Este tipo de organizaciones necesita dotarse de fondos para poder solventar todas sus operaciones, incluido su brazo militar, las Brigadas Al-Qassam. Si bien el grueso de sus fondos provendría de ayuda económica estable, de Estados u organizaciones no gubernamentales, el grupo siempre está en búsqueda de personas que deseen colaborar con sus objetivos. Es, a partir de estas donaciones, que se expresa el vínculo con las nuevas tecnologías financieras (Departamento de Justicia de los Estados Unidos de América, 2020).

En los inicios de esta tecnología, cuando todavía era una actividad de un grupo reducido de especialistas, algunos grupos terroristas empezaron a aprovechar las características propias

que este tipo de activos presentaban, entre otras, el anonimato, la celeridad y su facilidad para eludir los controles gubernamentales en la economía legal. Inicialmente se presentaban en redes sociales sosteniendo una pancarta, donde ofrecían la posibilidad de ayudar a su causa a través de las donaciones en Bitcoin. Para ello, allí mismo informaban los datos de una clave pública vinculada a una billetera que sería de su titularidad. Sin embargo, con el correr del tiempo, este proceder les quitaba el anonimato y volvía íntegramente trazables todas las operaciones. Los servicios de inteligencia de los diferentes países podían fácilmente realizar una trazabilidad histórica y rastrear a sus financistas (Wilson y Williams, 2019).

Una segunda etapa, en esta búsqueda de fondos por parte de la organización, fue la utilización de los servicios de mensajería instantánea y foros de redes sociales, en los cuales se realizaban posteos requiriendo donaciones. Pero, en este caso, en vez de postear una dirección de *clave pública*, indicaban que debían ingresar a un sitio web en la red oscura, mejor conocida como TOR (Blanco, 2020), donde se generaría una nueva *clave exclusiva* para cada donación. En la Figura N° 1 podemos observar una representación gráfica de este proceder (Elliptic, 2021).

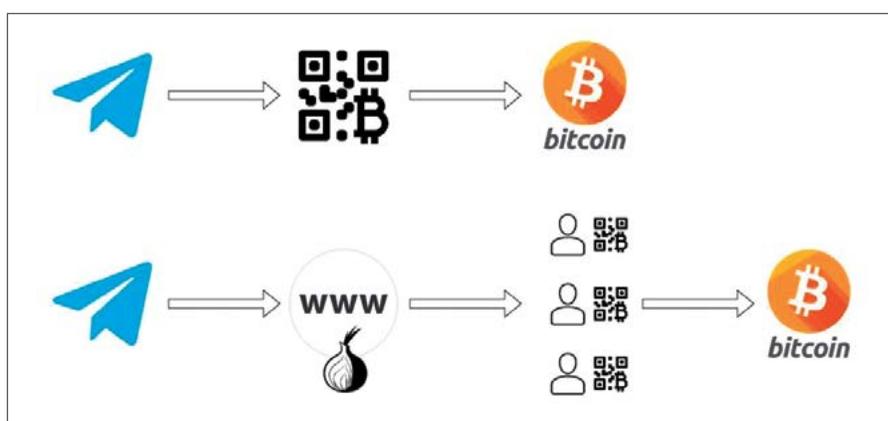


Figura N° 1. Esquema sobre cómo fueron los dos métodos de recaudación utilizados por las brigadas Al-Qassem. Fuente: Elaboración propia.

Desde el punto de vista de una investigación, esto le añade una capa de complejidad significativa a la trazabilidad de las operaciones. Antes existía una sola dirección hacia donde fluían todos los fondos, quedando informadas, gracias a la *Blockchain*, todas las claves públicas desde donde salían los fondos. Era cuestión de requerir información a las diferentes plataformas de compra-venta de criptoactivos hasta dar con la persona humana asociada a la misma.

Pero, con la implementación de este nuevo método, la complejidad crece doblemente:

- Por un lado, la utilización de TOR (*The Onion Router*, por su nombre en inglés) para acceder a un sitio web en la *dark web*. En pocas palabras, este es un software libre que genera una red abierta que permite a los usuarios navegar por internet de forma anónima al encriptar su tráfico de internet, enviándolo a través de múltiples servidores (cada servidor solo podrá ver la dirección IP del servidor anterior y siguiente en la cadena de comunicaciones), lo que hace que sea extremadamente difícil rastrear la actividad en línea de un usuario.

- Por otro lado, determinar la clave pública asociada al grupo terrorista crece exponencialmente, pues se generará una clave pública por cada donación que se realiza, haciendo que determinar su trazabilidad sea un trabajo herculeano.

En el mejor de los casos, se dará con los fondos —si se obtiene información de alguna plataforma o de un Reporte de Operación Sospechosa a través de una Unidad de Información Financiera— solo cuando se liquiden los fondos, con torpeza, en un país colaborador. Este es el caso de lo ocurrido con las brigadas Al-qassem, ya que, a través de diferentes agencias gubernamentales de los Estados Unidos, se logró detener este proceder y así decomisar los fondos recibidos en criptoactivos por dicha organización (Santos, 2020; Philipps, 2020; Strohm, 2020).

B. TOMA DEL CONGRESO DE EE.UU.

El 6 de enero de 2021, se llevó a cabo una violenta insurrección en el Capitolio de los Estados Unidos en Washington D.C., ocurrió mientras el Congreso certificaba los resultados de las elecciones presidenciales de 2020 en las cuales Joe Biden había sido electo como presidente de los Estados Unidos de Norteamérica. Dicha acción fue liderada por partidarios del entonces presidente Donald Trump, quienes habían sido convocados para una manifestación en apoyo a las afirmaciones que denunciaban un fraude electoral (Biesecker *et al.*, 2021). El Congreso se suspendió temporalmente y los legisladores fueron evacuados del edificio. Los manifestantes lograron ingresar a la sede del Senado y la Cámara de Representantes, ocupando las oficinas de algunos legisladores y causando daños en varias partes del edificio (BBC News, 2021).

La policía finalmente recuperó el control del Capitolio después de varias horas y se reportaron varios heridos y muertos, incluyendo un oficial de policía. La insurrección fue condenada por líderes políticos de todo el mundo y resultó en el segundo *impeachment* contra Trump por “incitación a la insurrección”.

A priori, parece que este caso no tiene mucho en común con el analizado en el punto anterior. Sin embargo, existe un detalle en común: el financiamiento se habría realizado a través del uso de criptoactivos. Fue gracias a la trazabilidad que facilita la operatoria de criptomonedas que la compañía Chainalysis logró probar pagos en criptoactivos —por 500.000 dólares— a los simpatizantes más radicalizados de Trump, pagos presuntamente provenientes de grupos de extrema derecha de Francia (Nelson, 2021; Lambe, 2021).

Conclusión Así, los dos casos mencionados en el apartado anterior dan cuenta de los beneficios que tienen los criptoactivos en el marco del delito de financiamiento del terrorismo, aunque la pregunta es: ¿beneficio para el financiador o para el investigador?

Cualquier operación de este estilo conlleva una gran preparación, en especial, insume fondos y tiempo. Ambas condiciones se interrelacionan, por lo que la falta de una de ellas truncará el desarrollo y progreso de dichas operaciones. En ese sentido, y tal como surge de los dos casos analizados, la utilización de los criptoactivos como herramienta de financiación del terrorismo sin dudas presenta beneficios, en especial, la circunvalación de los controles estatales en el mundo bancario-financiero, y la celeridad en la llegada de los fondos.

Sin embargo, si el grupo terrorista no es rápido en su accionar, no habrá financiamiento en criptoactivos alguno que prevenga su desarticulación por los servicios gubernamentales. El rastro de evidencia que deja en su paso puede ser un problema, en el sentido que, si el grupo y/o su financiador se encuentran bajo investigación, será relativamente sencillo realizar una trazabilidad de los fondos. Su condición digital, en ambos casos, es lo que genera estas ventajas para ambas partes.

Recordemos que el criminal —ya sea un narcotraficante o una persona intentando lavar fondos provenientes de un ilícito, o mismo el terrorista— no desea los criptoactivos en sí mismos, sino el dinero en efectivo que obtendrá de su liquidación. Los criptoactivos no son más que herramientas, hasta poder hacerse del verdadero activo anónimo, el dinero en efectivo.

Vale la pena recordar la conclusión de Micheal Morell, ex Director de la Agencia Central de Inteligencia de los Estados Unidos. Al estudiar la vinculación de la criminalidad compleja y la utilización de los criptoactivos, concluye que existe una sobreestimación del vínculo que hay entre ambas dimensiones, enfatizando respecto al bajo nivel de comprensión del valor sustancial de la *blockchain* como herramienta analítica para lograr avanzar en las investigaciones que requieran una trazabilidad de fondos (Morell *et al.*, 2021). Con las herramientas apropiadas de trazabilidad y un entendimiento de la tecnología, es claro que los criptoactivos en el contexto del financiamiento del terrorismo —aunque de cualquier delito— serán los mejores aliados de los investigadores.

Bibliografía

- Aboso, G. E. (2019). *Código Penal de la República Argentina. Comentado, concordado con jurisprudencia* (5ta ed.). Buenos Aires: Editorial B de F.
- Adams, M. y Curry, B. (18 de marzo de 2023), Who is Satoshi Nakamoto? *Revista Forbes*. <https://www.forbes.com/advisor/investing/cryptocurrency/who-is-satoshi-nakamoto/>
- BBC News. (6 de enero de 2021). US Congress in turmoil as violent Trump supporters breach building. *BBC News*. <https://www.bbc.com/news/world-us-canada-55555074>
- Biesecker, M.; Kunzelman, M.; Flaccus, G. y Mustian, J. (11 de enero de 2021). Who were they? Records reveal Trump fans who stormed Capitol. *AP News*. <https://apnews.com/article/us-capitol-siege-trump-supporters-8edfd3bb994568b7cdcd2243ad769101>
- Blanco, H. (2020), *Tecnología informática e investigación criminal*. Buenos Aires: Editorial La Ley.
- Blanco Cordero, I. (2015). *El delito de blanqueo de capitales*. Pamplona: Editorial Thomson Reuters-Aranzadi.
- CHAINALYSIS (17 de enero de 2020). Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly. <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-and-Terrorism.pdf>
- Departamento de Justicia de los Estados Unidos de América (13 de agosto de 2020). Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Largest Ever Seizure Of Terrorist Organizations' Cryptocurrency Accounts. *Comunicado de Prensa Nº 20-773*. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>
- Elliptic (3 de junio de 2021). Elliptic Identifies Surge in Bitcoin Donations to Hamas-Linked Terror Group. <https://www.elliptic.co/blog/surge-in-bitcoin-donations-to-hamas-linked-terror-group>
- Eraso Lomaquiz, S. (2015). *Las monedas virtuales en el Derecho argentino. Los Bitcoins*. La Ley.

- Faucon, B.; Talley, I. y Said, S. (2021). Israel-Gaza Conflict Spurs Bitcoin Donations to Hamas. *The Wall Street Journal*. <https://www.wsj.com/articles/israel-gaza-conflict-spurs-bitcoin-donations-to-hamas-11622633400>.
- FINMA (2018) Eidgenössische Finanzmarktaufsicht FINMA. *FINMA Annual Report 2018*, p. 30. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>
- Lambe, J. (14 de febrero de 2021). Far-Right Extremists Received High-Value Bitcoin Donations Ahead of Capitol Riots From Possibly-Deceased French Donor. *Law&Crime*. [Bitcoin Donations to Far-Right Groups May Have Funded Capitol Riot \(lawandcrime.com\)](https://www.lawandcrime.com/news/bitcoin-donations-to-far-right-groups-may-have-funded-capitol-riot/)
- Maldonado, J. (10 de septiembre de 2020). ¿Qué es un Exchange? *Cointelegraph*. <https://es.cointelegraph.com/explained/what-is-an-exchange>
- Merger, K. (1892). El origen del dinero. *The Economic Journal*, 2(6), 239-255. <https://doi.org/10.2307/2956146>.
- Morell, M.; Kirshner, J. y Schoenberger, T. (2021). An Analysis of Bitcoin's Use in Illicit Finance. *Beacon Global Strategies*. <https://crypto4innovation.org/wp-content/uploads/2022/07/An-Analysis-of-Bitcoins-Use-in-Illicit-Finance-By-Michael-Morell.pdf>
- Nabot, D. (13 de julio de 2018). Triple Frontera: congelan bienes de una organización vinculada a Hezbolla. *La Nación*. <https://www.lanacion.com.ar/politica/triple-frontera-congelan-bienes-de-una-organizacion-vinculada-a-hezbollah-nid2152501/>
- Nakamoto (30 de diciembre de 2019). The Cypherpunks. <https://nakamoto.com/the-cypherpunks/>
- Nelson, D. (14 de junio de 2021). Alt-Right Groups Received \$500K in BTC Month Before Capitol Riot: Chainalysis. *CoinDesk*. <https://www.coindesk.com/alt-right-groups-received-500k-in-btc-month-before-capitol-riot-chainalysis>
- Oficinas de las Naciones Unidas contra la Droga y el Delito (UNODC) (s.f.). Terrorist Financing. <https://www.unodc.org/unodc/en/money-laundering/overview.html>.
- Philipps Erbs, K. (13 de agosto de 2020). IRS-CI Involved In Largest-Ever Seizure Of Terrorist Organizations' Cryptocurrency Accounts. *Forbes*. <https://www.forbes.com/sites/kellyphillipserb/2020/08/13/irs-ci-involved-in-largest-ever-seizure-of-terrorist-organizations-cryptocurrency-accounts/?sh=582d8f102740>
- Pieralisi, M.; Corona Malano, F. N.; Rubiales, M. S. y Villalobos, N. M. (2018). *Normativa vigente en la República Argentina sobre Lavado de Activos de Origen Delictivo y Financiación del Terrorismo. Lineamientos generales para futuras modificaciones para CPN*. Universidad Nacional de Cuyo, Facultad de Ciencias Económicas. <https://bdigital.uncu.edu.ar/fichas.php?idobjeto=14833>
- Ramlall, I. (2013). "The impact of the subprime crisis on global financial markets, banks and international trade: a quest for sustainable policies" (trad.: "El impacto de la crisis subprime en los mercados globales financieros, bancario y comercio internacional: búsqueda de políticas sustentables"). Cambridge Scholars Publishing. <https://ebookcentral-proquest-com.dcu.idm.oclc.org/lib/dcu/reader.action?docID=1810292>.
- Santos, M. (2020). *Decomiso de cryptoactivos [Seizure of cryptoassets]*. Buenos Aires.
- Silva, G.; Feser, M. E.; Santos, M. y Ferreira, J. (2022). Criptomonedas y delitos complejos: hacia una nueva perspectiva de su impacto en la investigación criminal. *Revista Minerva. Saber arte y técnica*, VI(II), 6-19.

Strohm, C. (2020). U.S. Seized Cryptocurrency From Three Terrorist Groups *Bloomberg*. <https://www.bloomberg.com/news/articles/2020-08-13/u-s-says-it-seized-cryptocurrency-from-three-terrorist-groups#xj4y7vzkg>

Teichmann, F. M. J. (2018), "Financing terrorism through cryptocurrencies – A Danger For Europe?". *Journal of Money Laundering Control*, 21(4), 513-519. <https://www.emerald-com.dcu.idm.oclc.org/insight/publication/issn/1368-5201>

Wilson, T. y Williams, D. (26 de abril de 2019). Hamas Shifts Tactics In Bitcoin Fundraising, Highlighting Crypto Risks: Research. *Reuters*. <https://www.reuters.com/article/us-cryptocurrencies-hamas-idUSKCN1S20FA>

Zocaro, M. (2022). *Manual de Criptomonedas*. Osmar D. Buyatti Librería Editorial.

Cita Sugerida: Santos Mailland, M. (2023). Financiamiento del Terrorismo 2.0: el uso de criptoactivos para financiar operaciones terroristas. *Minerva. Saber, arte y técnica*, VII (I). Instituto Universitario de la Policía Federal Argentina (IUPFA), pp. 6-17.

***SANTOS MAILLAND, MANUEL**

Abogado y Mg. en Derecho Penal, Universidad Austral. Actualmente cursando el Master Europeo en Datos, Derecho e Inteligencia Artificial (EMILDAI), beca completa del programa Erasmus Mundus+ de la Union Europea, en Dublin City University (DCU). Cuenta con certificación en Cryptocurrencies (LSE) y en Compliance (IAE). Ha trabajado en la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP) y en la PROCELAC en el área de Lavado de dinero, ambos del MPF.