



**Universidad**  
Zaragoza



# Trabajo Fin de Máster Abogacía

Dictamen elaborado por  
Darío Zuza Gamba

Con objeto de analizar desde una perspectiva penal el uso ilícito de las criptomonedas en el ámbito de la delincuencia organizada para la comisión de delitos económicos

Director:  
José Félix Muñoz Soro

Facultad de Derecho  
Enero de 2023

## ÍNDICE

I.	<b>INTRODUCCIÓN</b> .....	<b>4</b>
II.	<b>ESCRITO DE ACUSACIÓN</b> .....	<b>10</b>
	PRIMERO. - ANTECEDENTES DE HECHO .....	10
	SEGUNDO. - FUNDAMENTOS JURÍDICOS .....	28
	A) Del delito de organización criminal .....	28
	B) Del delito de estafa hiperagravada .....	32
	C) Del delito de blanqueo de capitales.....	43
	D) Del delito de falsedad documental .....	55
	E) Del delito de defraudación de fluido eléctrico .....	57
	TERCERO. – CIRCUNSTANCIAS MODIFICATIVAS DE LA RESPONSABILIDAD PENAL .....	58
	CUARTO. - CONCLUSIONES.....	58
III.	<b>REFERENCIAS</b> .....	<b>61</b>
	A) Legislación aplicable .....	61
	B) Bibliografía .....	62
	C) Jurisprudencia .....	63

## Agradecimientos:

Quisiera agradecer a mi tutor, José Félix Muñoz Soro, la deferencia demostrada al acoger mi propuesta sobre el presente trabajo, sus constantes recomendaciones y consejos y las molestias que durante los últimos ocho meses se ha tomado a la hora de encauzar mis esfuerzos en la dirección correcta.

Por último, quisiera agradecer a mis padres, José Fermín y Mari Carmen, por todo el cariño, el amor y el apoyo que durante los últimos años me han dado. Nada, absolutamente nada, habría sido posible sin vosotros. Espero que la vida me depare el tiempo suficiente necesario para compensaros todos vuestros esfuerzos que, os aseguro, no han sido en vano.

*En resumen lo digo, entiéndelo mejor:  
el dinero es del mundo el gran agitador,  
hace señor al siervo y siervo hace el señor;  
toda cosa del siglo se hace por su amor*

Arcipreste de Hita, Libro del Buen Amor

## I. Introducción

Si bien llevan más de una década siendo objeto de intercambio y especulación, no deja de ser cierto que las criptomonedas se encuentran hoy en día en un completo limbo jurídico.<sup>1</sup> Podemos afirmar sin temor a equivocarnos que los legisladores nacionales han fracasado en la mayoría de los casos a la hora de producir un sistema normativo que legisle debidamente la emisión, intercambio y operaciones con monedas creadas a través de la tecnología *blockchain* (verdadera alma máter de toda criptomoneda funcional).

No obstante lo anterior, existen precedentes jurisprudenciales que de modo cauteloso y parcial han tratado de arrojar algo de luz sobre este ámbito novedoso y alegal. Así, en una sentencia única en la materia que trata, el Tribunal de Justicia de la Unión Europea afirmó que el Bitcoin (la primera criptomoneda emitida y aceptada de forma generalizada) era una «divisa virtual de flujo bidireccional [...] que no tiene ninguna finalidad distinta de la de ser un medio de pago» y que las operaciones de intercambio de Bitcoins por moneda fiduciaria «no están comprendidas en el concepto de entrega de bienes [...] sino de prestaciones de servicios» y que como tales estaban sometidas al Impuesto del Valor Añadido.<sup>2</sup>

El Tribunal Supremo, por su parte, en su sentencia 326/2019 de 20 de junio afirmaba que «el bitcoin no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin».<sup>3</sup>

Sin embargo, estas aproximaciones jurisprudenciales han recaído más bien en un ámbito mercantil en el que el objeto del litigio orbitaba no tanto en cuanto al uso que se le podía dar a las criptomonedas sino en cuanto a la definición y consideración legal de la más representativa de ellas. El Parlamento Europeo fue algo más precavido al plasmar

---

<sup>1</sup> Con el fin de evitar malentendidos ligados a la sobreexplotación de términos, ha de precisarse que las criptomonedas, genéricamente hablando, son un tipo de moneda virtual y que las monedas virtuales son a su vez una clase de dinero electrónico

<sup>2</sup> Sentencia de 22 de octubre de 2015, Skatteverket c. David Hedqvist, C-264/14, EU:C:2015:718, apartado 12 Disponible [online] en: <https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=ES> (Fecha de consulta: 27 de diciembre de 2022)

<sup>3</sup> STS 326/2019 de 20 de junio, FJ 3º (ECLI:ES:TS:2019:2109)

en su Resolución de 26 de mayo 2016 sobre monedas virtuales una serie de riesgos vinculados a este tipo de activo entre las que se encuentran «la ausencia de estructuras de gobernanza flexibles, [...] una elevada volatilidad, [...] inseguridad jurídica [...] y las posibilidades de realizar operaciones en el mercado negro, blanqueo de dinero, financiación del terrorismo, fraude y evasión fiscal y otras actividades delictivas basadas en la pseudonimia y la combinación de servicios que ofrecen algunos de estos servicios y la naturaleza descentralizada de algunas monedas virtuales, habida cuenta de que la trazabilidad de las operaciones en efectivo tiende a ser muy inferior»<sup>4</sup>.

El Parlamento Europeo incidía de este modo en un aspecto fundamental de las criptomonedas como es su potencial uso ilícito o con una finalidad ilícita. Y es que, si bien no son reconocidas legalmente como tal, las criptomonedas cumplen estrictamente con las tres funciones del dinero: sirven en primer lugar como reserva de valor, pudiendo su titular atesorarlas con la seguridad de que en el futuro conservarán un valor que podrá o no fluctuar, sirven en segundo lugar como medio de cambio para adquirir bienes y servicios y sirven finalmente como unidad de cuenta que permite al titular adscribir un determinado valor específico al ente monetario. De este modo, podemos colegir que en tanto que dinero las criptomonedas podrán tener el mismo uso que aquel, y si el dinero real puede ser objeto de usos ilícitos también podrán serlo las criptomonedas. No en vano PÉREZ MEDINA afirma que los usos ilícitos de las criptomonedas están vinculados a cuatro áreas criminológicas diferenciadas: el blanqueo de capitales, la financiación del terrorismo, los delitos fiscales y la adquisición de bienes y servicios ilícitos en el ciberespacio.<sup>5</sup>

De esta forma, la realidad ha evidenciado reiteradamente que desde la implementación de las criptomonedas y su aceptación por el público como dinero éstas han sido utilizadas en numerosas ocasiones con fines delictivos. Así, se ha demostrado que el Estado Islámico y Al Qaeda han utilizado cupones de criptomonedas canjeables para enviar fondos desde Francia hasta Siria<sup>6</sup>, que numerosas organizaciones criminales

---

<sup>4</sup> Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre Monedas Virtuales (2016/2007 (INI)) Disponible [online] en: [https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228\\_ES.html](https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_ES.html) (Fecha de consulta: 27 de diciembre de 2022)

<sup>5</sup> PÉREZ MEDINA, D., «Blockchain, Criptomonedas y los Fenómenos Delictivos: entre el Crimen y el Desarrollo», en *Boletín Criminológico del Instituto Andaluz Interuniversitario de Criminología*, Edición Especial, n.º. 206, 2020, p. 10

<sup>6</sup> Deutsche Welle: Policía Francesa Detiene a 29 Personas por Financiar Terrorismo en Siria, 29 de septiembre de 2020. Disponible [online] en: <https://www.dw.com/es/polic%C3%ADa-francesa-detiene-a-29-personas-por-financiar-terrorismo-en-siria/a-55095768> (Fecha de consulta: 27 de diciembre de 2022)

ligadas a la delincuencia del este utilizan monederos físicos o *wallets frías* para acumular y desplazar con facilidad elevadas cantidades de criptomonedas que posteriormente canjean para su inversión en el mercado legal<sup>7</sup> o que a menudo el único modo de efectuar transacciones en los portales alojados en la *Dark Web* es a través de envíos de criptomonedas a las direcciones que integran los *escrows* que los administradores de las plataformas y canales de distribución ilícitas gestionan.<sup>8</sup>

Esta deriva criminalística de las criptomonedas basada en las facilidades que ofrecen para la perpetración de ilícitos penales fue entre otras la causa de la emisión por el Consejo y el Parlamento de la Unión Europea de la Directiva 2019/713 de 17 de abril sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo que recogía una definición del término «moneda virtual» e imponía a los Estados Miembros la obligación de trasponer a sus ordenamientos jurídicos medidas que garantizaran una prevención adecuada del blanqueo de capitales y de las operaciones ilícitas realizadas mediante el uso de monedas virtuales y monederos electrónicos.

El legislador español, cumpliendo con la obligación de trasponer la mencionada Directiva 2019/713 al ordenamiento jurídico nacional promulgó la LO 14/2022 de 22 de diciembre que supone a todas luces un paso fundamental en la legislación de las criptomonedas en nuestro país puesto que además de incorporar en el nuevo artículo 399 ter del Código Penal una definición de «medios de pago distintos del efectivo» menciona en su preámbulo su aplicabilidad a monedas virtuales, criptoactivos y monederos electrónicos. Igualmente, el incremento del riesgo de blanqueo de capitales a través de criptomonedas hizo motivó la reforma de la Ley 10/2010 de 28 de abril de prevención de

---

<sup>7</sup> Sirva como ejemplo el desmantelamiento en diciembre de 2020 por el Cuerpo Nacional de Policía en cooperación con Europol una de parte de la estructura de blanqueo de capitales de una sección de los *Vory v Zakone*<sup>7</sup> en Alicante e Ibiza. La operación había comenzado en 2013 cuando se detectaron multimillonarias transferencias provenientes del Reino Unido, Emiratos árabes y Letonia (todas ellas jurisdicciones opacas y de baja o nula tributación) El dinero, procedente del tráfico de armas, drogas, personas y extorsiones, se invertía en los sectores del ocio, hostelería y construcción del Levante y en las Islas Baleares y el patrimonio resultante era administrado por los líderes del esquema, que habían logrado infiltrar la Administración pública a través de agentes de policía y funcionarios de inmigración corruptos, contando con el asesoramiento de un despacho de abogados. En los registros efectuados se detuvo a 23 personas y además de intervenir un verdadero arsenal de guerra, 300,000 euros en efectivo y varias decenas de diamantes, se incautó una cantidad indeterminada de criptoactivos contenidos en monederos virtuales. Fuente: ABC, «La mafia rusa en Alicante una red clientelar de agentes, funcionarios y ediles», 17 de diciembre de 2020. Disponible [online] en: [https://www.abc.es/espana/abci-mafia-rusa-tenia-alicante-clientelar-agentes-funcionarios-y-ediles-202012162125\\_noticia.html](https://www.abc.es/espana/abci-mafia-rusa-tenia-alicante-clientelar-agentes-funcionarios-y-ediles-202012162125_noticia.html) (Fecha de consulta: 27 de diciembre de 2022)

<sup>8</sup> TSUCHIYA, Y., «Measuring Dark WebMarketplaces via Bitcoin Transactions: From Birth to Independence», en *Forensic Science International: Digital Investigation*, mayo de 2020

blanqueo de capitales y financiación del terrorismo añadiendo a través del Real Decreto Ley 7/2021 las definiciones de lo que se entiende por moneda virtual, cambio de moneda virtual por moneda fiduciaria y proveedores de servicios de custodia de monederos electrónicos, además de configurar a los «proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos» como sujetos obligados.

Es pues desde esta óptica a partir de la cual pretendo con el presente Trabajo de Fin de Máster analizar un supuesto de hecho en el que una serie de individuos, puestos de común y mediante el reparto de roles específicos, perpetran una serie de delitos que tienen las criptomonedas como línea vertebradora procediendo al mismo tiempo a la calificación jurídica de las distintas conductas presentes en los hechos. Debido a las características de la tarea he optado por adecuar un dictamen clásico al formato de un escrito de acusación elaborado por el Ministerio Fiscal en el entendimiento de que los elementos del primero (antecedentes de hecho, cuestiones planteadas, fundamentos jurídicos y conclusiones) son compatibles con los del segundo (fundamentos de hecho, calificación y fundamentación jurídica, fundamentos de derecho y conclusiones). Se trata, en suma, del análisis de una estafa clásica de tipo piramidal que utiliza la minería de criptomonedas como elemento engañoso para inducir a error a una amplia gama de clientes a facilitan distintas cantidades de dinero que son legitimadas por los miembros de la trama a través de un mecanismo cuya popularidad se ha incrementado recientemente; la transformación de los activos a través de su conversión en distintos tipos de criptomonedas. PÉREZ LÓPEZ ha hecho referencia a este mecanismo al calificarlo como «una de las opciones más interesantes para los blanqueadores y más disruptivas para su persecución (dada su sencillez, su eficacia en términos de costes en comparación con otros métodos y las dificultades técnicas asociadas a su trazado y evitación por las autoridades)” consistente en “ el mero envío de los tokens [las criptomonedas en sí] a paraísos fiscales para su cambio en moneda de curso legal por *exchangers* locales y su reintroducción en el sistema financiero internacional».<sup>9</sup>

Considero importante remarcar el hecho de haber optado por analizar la confluencia de los individuos intervinientes bajo el prisma de una organización criminal,

---

<sup>9</sup> PÉREZ LÓPEZ, X., «Las Criptomonedas: Consideraciones Generales y Empleo de las Criptomonedas Como Instrumento de Blanqueo de Capitales en la Unión Europea y en España», en *Revista de Derecho Penal y Criminología*, 3ª Época, nº. 18, julio de 2017, págs. 141-187

puesto que el fenómeno asociativo de los artículos 570 bis y 570 ter CP está siendo cada vez más utilizado por los Tribunales nacionales a la hora de enjuiciar las numerosas estafas de tipo piramidal que utilizan el mundo de las criptomonedas como plataforma de engaño. No nos encontramos ya con un empresario carismático que se vale de su perfil y crédito profesional para estafar a cierto número de inversores engañándoles para invertir en un fraude piramidal ligado a la filatelia ni a holdings gestionados por un clan familiar sino con organizaciones jerarquizadas y grupos de individuos que pergeñan una estrategia mediante el reparto de roles especializados y en el que el blanqueo de capitales internacional juega un papel preponderante.<sup>10</sup> No en vano la Memoria de la Fiscalía General del Estado relativa al año 2021 afirmaba que los ciberdelitos se habían incrementado en un 40,47% con respecto al 2020 (pasando de 16.914 procedimientos a 23.801) y un 257% en comparación con el año 2017 en que se comenzó a compilar la estadística de delitos cometidos a través de TICs, constituyendo de entre todos ellos las estafas en línea un considerablemente notable 75,5% del total (17.969 casos).<sup>11</sup> En esta línea, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023 establecía la necesidad de apreciar la evolución en las técnicas de blanqueo de capitales empleadas por la criminalidad organizada citando expresamente las criptomonedas como una nueva modalidad.<sup>12</sup>

Por ello, he tratado de reflejar en el caso analizado una metodología similar en la que las ganancias sustraídas a las víctimas de la estafa son canalizadas a través de cuentas bancarias aperturadas de forma telemática utilizando documentación ajena —algo muy común en el marco de la cibercriminalidad— para la compra de criptomonedas a través de casas de cambio ubicadas en jurisdicciones opacas en donde la nula cooperación judicial

---

<sup>10</sup> *Exempli Gratia*, durante la redacción del presente TFM tuvo amplia repercusión en España la disrupción de una organización criminal que desde Albania había estafado mundialmente alrededor de 2.400 millones de euros (contándose 17.000 afectados en nuestro país) mediante inversiones en esquemas de trading de criptomonedas inexistentes. Véase: Europa Press, «Desmantelado en Albania un presunto grupo que ganó 2.400 millones en estafas con criptomonedas falsas» Disponible [online] en: <https://www.europapress.es/catalunya/noticia-desmantelado-albania-presunto-grupo-gano-2400-millones-estafas-criptomonedas-falsas-20221114131640.html> (Fecha de consulta: 28 de diciembre de 2022)

<sup>11</sup> Memoria Elevada al Gobierno de S.M., Capítulo III, Apartado 8, Fiscalía Especializada contra la Criminalidad Informática. Disponible [online] en: [https://www.fiscal.es/memorias/memoria2022/FISCALIA\\_SITE/index.html](https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/index.html) (Fecha de consulta: 28 de diciembre de 2022)

<sup>12</sup> 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. Disponible [online] en: [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2019-2442](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442) (Fecha de consulta: 28 de diciembre de 2022)



posibilita el blanqueo de capitales a través de casas de cambio que operan bajo un control legal mínimo cuando no inexistente.

Otra de las especialidades que he optado por incluir en el presente trabajo ha sido la utilización de medidas de investigación tecnológicas previstas en el Título VIII del Libro II LECRIM -fundamentalmente intervenciones telefónicas y registros remotos a dispositivos de almacenamiento masivo de información- para ilustrar la utilidad que semejantes diligencias pueden aportar a las investigaciones de organizaciones criminales que cometen buena parte de su actividad delictiva en el ciberespacio. En este caso, una parte importante de la actividad probatoria recae, como se verá, en la interceptación de llamadas telefónicas de miembros de la organización localizados a través de la numeración IMEI así como en el rastreo del portátil utilizado por el blanqueador para transferir sumas de dinero entre diferentes cuentas bancarias identificándolo merced a la dirección MAC. Este tipo de medidas de investigación son fundamentales en la investigación y interrupción de las actividades de la delincuencia organizada y como tales me ha parecido necesario incluirlas en un caso en el que el aspecto tecnológico es esencial.

En conclusión, el presente Trabajo de Fin de Máster pretende simular y al mismo tiempo analizar la creación, funcionamiento y interrupción de las actividades de una organización criminal que utilizando las criptomonedas como instrumento de engaño opera una estafa piramidal de considerables proporciones utilizando igualmente los criptoactivos como método de blanqueo de las ganancias. Con ello he tratado de hacer énfasis en el riesgo que este tipo de casos —cada vez más frecuentes, todo sea dicho— suponen en el panorama de la delincuencia organizada económica española e internacional y en el modo en que, en el ámbito procesal, puede hacerseles frente. Queda al arbitrio de quien lea estas líneas concluir si he obrado o no de modo adecuado para lograrlo.

## II. Escrito de acusación

### AL JUZGADO

**EL FISCAL**, despachando el trámite previsto en el artículo 780 de la Ley de Enjuiciamiento Criminal, solicita la apertura de juicio oral ante la **SALA DE LO PENAL DE LA AUDIENCIA NACIONAL**, formulando **ESCRITO DE ACUSACIÓN** contra **VITALY VLADIMIROVICH NASTANIEK, ANTONIO SÁENZ DE SUESCUN y JAVIER GÓMEZ RUPÉREZ**, en base a las siguientes **CONCLUSIONES PROVISIONALES**:

#### **PRIMERO. – Antecedentes de hecho**

**1ª.-** Los acusados **VITALY VLADIMIROVICH NASTANIEK**, abogado de profesión colegiado con el N° 60.674 con DNI 84.576.63 M y sin antecedentes penales, **ANTONIO SÁENZ DE SUESCUN**, con DNI 54.562.615 Z y sin antecedentes penales computables a efectos de reincidencia en la presente causa, y **JAVIER GÓMEZ RUPÉREZ**, con DNI 92.567.174 G y sin antecedentes penales, puestos de común acuerdo y con la finalidad de obtener un lucro ilícito constituyeron una organización criminal dedicada a la extracción de rentas a través de un entramado defraudatorio basado en la oferta de servicios de inversión en criptomonedas realizando los siguientes hechos:

**ANTONIO SÁENZ DE SUESCUN**, prevaliéndose de su credibilidad y prestigio profesional derivado del hecho de ser un conocido empresario que adquirió notoria fama durante junio de 2016 al aparecer en numerosos canales de televisión de alcance nacional siendo consultado en calidad de experto en mercados financieros y tendencias del mercado de valores fundó el 7 de julio de 2021 en Estonia la mercantil **CRYPTO INVERSIÓN LIMITED** con una inversión inicial de 300 euros divididos en un total de 100 participaciones de las que él era el único titular. La mercantil tenía como domicilio el n° 50 de la calle Boorkusplats de la ciudad de Tallín (Estonia) y tal y como consta en su escritura de constitución (obtenida a través de la Orden Europea de Investigación de fecha 27 de julio de 2022 adjuntada como Documento n° 1 en la relación de documentos que acompañan al presente escrito merced a la información suministrada por la unidad de delitos tecnológicos de la Politsei Ja Piirivalveamet estonia) se constituyó por vía

telemática por intermediación de **CORPORATE CREATOR LIMITED**, una empresa estonia de incorporación de empresas *offshore*, a través de una transacción por valor de 300 euros mediante las cuales se contrataron los siguientes productos

- a) Apertura de la cuenta EE90 5412 3455 7384 5905 a nombre de **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK**
- b) Gestión de apartado de correos sito en el nº 50 de la calle Boorkusplats, Tallín, Estonia
- c) Preparación anual de declaración de impuestos y presentación de cuentas sociales ante organismos reguladores y fiscalizadores

Como se refleja en la documentación adjuntada en la Orden Europea de Investigación la mercantil **CRYPTO INVERSIÓN LIMITED** tenía por objeto social *“la elaboración, transformación, distribución y comercialización de productos electrónicos, tecnológicos e informáticos, la administración de locales, la promoción y organización de eventos así como la prestación, gestión y explotación de actividades de restauración y cocina a través de bares, restaurantes, cafeterías y bares en toda clase de establecimientos tanto de titularidad propia como en régimen de alquiler y/o franquicia”*. Como posteriormente se advertirá, la naturaleza eminentemente vaga y amplia del objeto de la mercantil **CRYPTO INVERSIÓN LIMITED** estaba concebida de antemano con la finalidad de facilitar en la medida de lo posible la operatividad del entramado defraudatorio constituido alrededor de esta persona jurídica. Por otro lado, el hecho de que la razón social de la empresa en torno a la cual orbita la trama objeto del presente escrito se ubique en Estonia no es casualidad. Es de sobra conocido el carácter relevante del país en el marco de la inversión de capitales en el entorno digital, tratándose del Estado miembro de la Unión Europea que mayor facilidades ofrece para la fundación de empresas tecnológicas a través de la denominada *e-Residency* en base a unas condiciones del todo opacas y ajenas a los más mínimos controles dirigidos a prevenir el fraude, el blanqueo de capitales y demás conductas ilícitas perpetradas a través de la instrumentalización de personas jurídicas.

La mercantil **CRYPTO INVERSIÓN LIMITED**, con los acusados **ANTONIO** (en calidad de propietario y sujeto visible) y **VITALY** y **JAVIER** (éstos últimos en calidad de asistentes y empleados de la empresa tal y como consta en los contratos de trabajo firmados el 7 de julio de 2021 y que se aportan en la relación de documentos

adjunta al presente escrito con los números 2 y 3) era el centro del esquema defraudatorio cuyo funcionamiento a efectos de captación de rentas tenía lugar del siguiente modo:

- I) A través de la mercantil **CRYPTO INVERSIÓN SRL** se ofertaba un mecanismo de inversión en criptomonedas a través de una plataforma online denominada **CRYPTOGOXX** dedicada a la creación, mantenimiento y explotación de *Masternodes* a través de una metodología de trabajo basada en la *Proof of Service* en el marco de la cadena de bloques o *Blockchain*.
  
- II) La idea fundamental de la tecnología *blockchain* descansa sobre el concepto matriz de descentralización. Contrariamente a los sistemas tradicionales de información en los que ésta se mantiene almacenada en nodos centrales o principales que regulan los flujos de entrada y salida logrando de esta forma controlar la cantidad de información a la que los usuarios pueden acceder el sistema de *blockchain* se basa en la descentralización más absoluta. Y es que de acuerdo con este sistema deja de haber nodos centrales al proceder cada uno de los integrantes del sistema o red a almacenar información por si mismo generando en comunidad con el resto de los nodos el sistema por entero. La base de la tecnología *blockchain* se fundamenta en las estructuras *Peer-to-Peer* o *P2P* en las que cada uno de los participantes forma parte integral de la estructura general, almacenando, recibiendo y compartiendo información con el resto de integrantes. Sin embargo, la tecnología *blockchain* va aún más allá del concepto simple de red *P2P*. No se trata simplemente de un sistema de información retroalimentado a través de la continua y exponencialmente creciente comunidad de participantes todos los cuales comparten la información que poseen; en realidad la tecnología *blockchain* se basa en la construcción de bloques de información (*blocks*) que van añadiéndose entre sí conectados por códigos (*hashes*) formando una cadena (*chain*) ininterrumpida que contiene toda la información del sistema. Los participantes (de acuerdo con la lógica básica de los sistemas *P2P*) tienen una copia de la información contenida en la cadena, que es completamente accesible. Por otro lado, los bloques se construyen a través de operaciones muy complejas denominadas pruebas de trabajo (*proof of work*) que pueden ser resueltas por los usuarios que así lo decidan. Una vez resuelta una determinada prueba de trabajo el

resultado obtenido es un bloque completo que se adiciona a la cadena preexistente planteándose a continuación una nueva prueba de trabajo para continuar con la construcción de un nuevo bloque, obteniendo en muchos casos el usuario que haya logrado resolver la prueba de trabajo una recompensa que adopta la forma de activo digital.

- III) En el marco general del mantenimiento de una cadena de bloques o *blockchain* son muchos los servicios o actividades que pueden ser objeto de explotación y por tanto de extracción de una cierta rentabilidad. Por ello, es alrededor de la idea de explotación de la *blockchain* que surge el concepto de *Masternodo* o *Masternode* como un segundo nivel de la cadena de bloques que opera en paralelo a ésta y que se dedica a realizar tareas que podríamos denominar de apoyo: albergar copias de la *blockchain* para garantizar la descentralización, verificación no del minado de bloques sino de las transacciones entre mineros y participar en la gestión general del sistema.

Estos servicios, ya de por sí ambiguos y complejos, son relativamente fáciles de explotar por entramados delictivos gracias a amplios sectores de inversores desinformados que confían en el funcionamiento de sistemas *blockchain* completamente opacos cuando no inexistentes.

- IV) Los acusados utilizaban la plataforma **CRYPTOGOXX** como canal de captación de inversores a quienes se hacía creer que la mercantil **CRYPTO INVERSIÓN LIMITED** gestionaba un sistema de explotación de *masternodos* cuyo funcionamiento les era expuesto de una forma simplificada y contradictoria a través de seminarios o reuniones colectivas tanto presenciales como online impartidas por el propio **ANTONIO**. Estos encuentros no eran fortuitos; por el contrario, todo cliente era alentado con la promesa de obtener beneficios adicionales a que atrajera a nuevos inversores. Las personas atraídas a la plataforma eran en su mayoría bien sujetos jóvenes en edad universitaria bien personas jubiladas (ninguna de ellas con conocimientos especializados en materia de inversiones financieras) a quienes se les hacía creer que el depósito de sus ahorros en el sistema defraudatorio era una buena forma de capitalizar las inversiones realizadas. En resumen, el sistema de captación de víctimas utilizado por la organización criminal integrada por los acusados se nutría de potenciales estafados a través de un sistema de patronazgo interiorizado y gestionado por las propias víctimas,

víctimas que eran precisamente seleccionadas tanto por su edad como por su inexperiencia de cara a facilitar el engaño.

- V) La inversión en el sistema de gestión de masternodos denominado **CRYPTOGOX** estaba sujeta a una inversión inicial mínima de 100 euros pagaderos por medio de transferencia llegando a ofrecerse medios alternativos de remisión de fondos aceptándose mecanismos como Bizum o PayPal. Todos los pagos habían de realizarse a la cuenta EE90 5412 3455 7384 5905 aperturada a nombre de **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK**. Para realizar esta inversión inicial el cliente debía cumplimentar un formulario facilitado en la página web de **CRYPTOGOX** ([www.cryptogox.ee](http://www.cryptogox.ee)) que adoptaba la forma de un contrato mediante el cual se asumía la obligación de no retirar los fondos hasta transcurridos 2 años desde la realización del pago. Igualmente, el contrato exigía la aportación de una dirección Ethereum para que **CRYPTOGOX** pudiera devengar las cuotas diarias. Para ello se instruía a los clientes para que se hicieran con un monedero o *wallet* con una dirección asociada que debía ser incorporada al contrato.
- VI) De acuerdo con la información suministrada en las conferencias impartidas por **ANTONIO** todo inversor recibía a partir del día de la transferencia original una rentabilidad diaria del 0,15% (un 4,5% mensual) extraída de la gestión de los masternodos. Estas cantidades eran giradas diariamente a las direcciones Ethereum aportadas por los clientes en sus contratos.
- VII) A efectos de administración de la inversión original (a la que se podían adicionar con posterioridad nuevos pagos con el fin de incrementar el monto inicial) ésta era dividida en dos fondos o *pools* del siguiente modo:
- Un 20% se destinaba a un *Bonus Pool* que devengaba remuneraciones individualizadas por cada nuevo inversor que los clientes de **CRYPTOGOX** atrajeran a la plataforma
  - Un 80% se destinaba a un *Operational Pool* dentro del cual el 70% se destinaba a sufragar los pagos diarios a los inversores, un 20% a gastos de mantenimiento y un 10% en calidad de beneficios retenidos por **CRYPTOGOX**.
- VIII) Como quiera que el esquema defraudatorio orbitaba en torno a la explotación de un sistema vinculado al mantenimiento de *masternodos*, los acusados

**ANTONIO, VITALY y JAVIER**, con la finalidad de mantener una apariencia lícita de negocio, realizaban los pagos a los clientes en forma de criptomonedas ingresando en principio las cantidades prometidas en concepto de bonus en los monederos virtuales cuyas direcciones facilitaban los clientes en el momento de ratificar el contrato con **CRYPTOGOX**. Los pagos en un principio se realizaban de modo regular, si bien las transacciones diarias se sufragaban con las aportaciones que los nuevos clientes ingresaban al sistema sin que hubiera ninguna actividad vinculada a la explotación de *masternodos* que generase un rendimiento suficiente para garantizar la cobertura de cuotas diarias. En resumen, las obligaciones de los acusados para con sus clientes se compensaban merced a las cantidades aportadas por nuevas víctimas, apreciándose en esta metodología un patrón propio de la estafa de tipo piramidal.

Las diligencias de investigación practicadas durante la instrucción del procedimiento que ha dado lugar a la interposición del presente escrito de acusación demostraron como las cantidades eran destinadas al lucro personal de **ANTONIO, VITALY y JAVIER** sin que en ningún caso se diera a los fondos recaudados conforme a lo expuesto *ut supra* la finalidad oficialmente pretendida.

La organización criminal integrada por **ANTONIO, VITALY y JAVIER**, con el fin de mantener las apariencias y simular una actividad comercial del todo inexistente decidieron rentar una nave industrial sita en el nº 30 del polígono industrial de Alfajarín (Zaragoza) en el que instalar una red de servidores supuestamente dedicados a la gestión de *masternodos*. En el contrato de arrendamiento figuraba como arrendatario **JAVIER**, quien era además el encargado de interactuar con el propietario de la nave y quien realizaba a través de una cuenta bancaria a su nombre los desembolsos correspondientes a las mensualidades, que se realizaban durante los primeros siete días de cada mes.

En su lugar, la organización, utilizando parte de los fondos obtenidos durante los meses de julio y agosto de 2022, el procesado **JAVIER** adquirió un total de 100 equipos ASIC (*Application-Specific Integrated Circuit*) Un equipo ASIC es un procesador que contrariamente a los tradicionales CPUs incorporados a todo sistema informático de uso común no está diseñado para la gestión de múltiples tareas mediante mecanismos de gestión de procesos a través de algoritmos de planificación como los usuales *Round Robin*, *Multi Level Queues*, *Shortest Remaining Time*, etc. Por el contrario, los

procesadores ASIC están diseñados para servir una única tarea en exclusiva. Es por ello que diseñados a partir de la tecnología FPGA los dispositivos ASIC han venido siendo utilizados para el minado de criptomonedas para lo cual requieren altas cantidades de energía eléctrica así como sistemas de refrigeración para atemperar las elevadas temperaturas generadas durante el proceso.

Con esta operación, la organización criminal integrada por **ANTONIO, VITALY** y **JAVIER** pretendía no solo justificar una explotación de *masternodos* inexistente (de lo cual se encargaba **ANTONIO** publicando de forma reiterada fotografías de la instalación en redes sociales haciéndola pasar por auténticos *masternodos* gestionados en Estonia) sino que además llevaba a cabo una mecánica real de minado de criptomoneda Bitcoin con una finalidad puramente lucrativa. Para ello accedieron de forma ilegal a la instalación eléctrica de la nave industrial puenteando los cables mediante el uso de regletas de clemas.

La actividad de la organización criminal integrada por **ANTONIO, VITALY** y **JAVIER** generaba unos ingresos que han sido estimados en alrededor de 25.000€ diarios y para conseguir no solo el enmascaramiento del tratamiento dado a éstos fondos sino también para generar un volumen de negocios que permitiera a los procesados interferir en la posible investigación de sus actividades éstos procedieron al diseño e implementación de un mecanismo de blanqueo del que se encargaba exclusivamente el procesado **VITALY**. El mecanismo seguía la siguiente lógica:

- I) Con el montante acumulado en la cuenta la cuenta EE90 5412 3455 7384 5905 a nombre de **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK** el procesado **VITALY** adquiría cantidades notables de la criptomoneda denominada Monero (XMR) Estas adquisiciones se hacían online a través de transacciones operadas vía servidores de numerosas casas de cambio que la Orden Europea de Investigación solicitada en el marco de la investigación que ha servido de base a este escrito de acusación ha localizado en Singapur y Hong Kong.
- II) La criptomoneda Monero (XMR), contrariamente a otros criptoactivos como Bitcoin o Ethereum se caracteriza por una mecánica de funcionamiento



especialmente diseñada para facilitar el anonimato.<sup>13</sup> De esta forma, si bien es posible rastrear el origen y destino de una transacción de por ejemplo, Bitcoins, cotejando los datos alojados en el sistema de bloques que es completamente público y que permite unir los dos elementos básicos de toda transacción, *input* (dirección de la que proceden los fondos) y *output* (dirección a la que se envían) en el caso de Monero (XMR) las transacciones utilizan un tipo de modalidad en anillo que mezcla dirección *input* y *output* ficticias a efectos de enmascarar las reales.<sup>14</sup> A esto se le debe sumar el uso del denominado protocolo *Ring Confidential Transactions* (RingCT) que oculta deliberadamente la cuantía de que se compone el *output* de toda transacción no permitiendo pues conocer la cantidad exacta de criptomonedas que se transfieren, excepción hecha de las monedas extractadas por los mineros (*coinbase*) que son plenamente rastreables con relación a su primer movimiento. De esta forma, en condiciones normales, no es posible garantizar con certeza la dirección de origen y de destino ni la cantidad exacta de ninguna transacción de Monero (XMR)<sup>15</sup>.

- III) Una vez convertidas en Monero (XMR), las cantidades originarias de la cuenta EE90 5412 3455 7384 5905 a nombre de **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK** eran de nuevo convertidas en dinero de curso legal o fiduciario recorriendo el camino inverso, es decir, vendiendo los criptoactivos a través de las mismas casas de cambio. Las sumas resultantes eran remitidas a tres cuentas bancarias

---

<sup>13</sup> Existe evidencia empíricamente contrastada acerca de la popularidad de Monero (XMR) en ámbitos de la criminalidad organizada vinculadas a redes de *cryptojacking* asiáticas que si bien exigen a las víctimas pago en Bitcoins utilizan casas de cambio registradas en Europa para tratar de romper el vínculo que facilite la trazabilidad de las transacciones. Un ejemplo paradigmático es el caso Wannacry, en el que el autodenominado Grupo Lazarus (vinculado al gobierno de la República Popular Democrática de Corea del Norte) infectó alrededor de doscientos mil equipos informáticos logrando cuanto menos blanquear 36.922 dólares obtenidos inicialmente en Bitcoins mediante su conversión en Monero a través de la casa de cambio suiza ShapeShift. Véase: MOSER, M. et al. «An Empirical Analysis of Traceability in the Monero Blockchain», en *Privacy Enhancing Technologies Symposium*, abril de 2018, ps. 15 y 16

<sup>14</sup> SEGURA RAMÍREZ, S., «Anonimato en blockchain: Monero», Trabajo de Final de Grado, Universitat Politècnica de Catalunya, julio de 2020, p. 21 y sigs Disponible [online] en: <https://upcommons.upc.edu/bitstream/handle/2117/327128/memoria.pdf?sequence=1&isAllowed=y> (Fecha de consulta: 15 de noviembre de 2022)

<sup>15</sup> SERHACK & MONERO COMMUNITY «Mastering Monero, the Future of Private Transactions», ps. 61 y sigs, 129 y sigs. Disponible [online] en: <https://masteringmonero.com/> (Fecha de consulta: 23 de noviembre de 2022, si bien desde entonces el documento ha sido objeto de restricción de acceso requiriéndose del pago de una cantidad para su obtención)

gestionadas por el acusado VITALY y aperturadas en la entidad financiera **ING** en España.

IV) Para ello el acusado **VITALY** adquirió a través de modo fraudulento respectivas copias de los Documentos de Identidad Personal (DNI) de los ciudadanos españoles **MARTÍN, GLORIA** y **SERGIO** procediendo a la alteración de las fotografías incluidas en los originales para utilizarlos junto a tres correos electrónicos creados al efecto (mart.Gonzmail@es, Glor.PerMar@.es y Serg.Enriq@.es) para aperturar de modo online las siguientes cuentas en la entidad financiera **ING**:

- Cuenta Nómina ING nº ES78 6475 5296 3659 6056 a nombre de **MARTÍN**
- Cuenta Nómina ING nº ES37 8267 7295 8294 5920 a nombre de **GLORIA**
- Cuenta Nómina ING nº ES92 7390 6185 2786 1896 a nombre de **SERGIO**

V) A continuación, **VITALY**, haciendo uso de una serie de personas cuya identidad no ha podido ser determinada, procedía a recolectar dinero en efectivo procedente de dichas cuentas utilizando para ello tarjetas de crédito y débito asociadas a las mencionadas cuenta utilizando para ello cajeros automáticos.

VI) Seguidamente, y utilizando para ello a las personas mencionadas, **VITALY** procedía a la adquisición de cupones **BITRATE** en numerosos puntos de venta. Estos cupones (que pueden adquirirse por cantidades de entre 25€ y 500€) son emitidos y administrados por la mercantil **BITRATE SA** que se encarga de adquirir en el mercado los bitcoins amparados por cada cupón. De este modo se requiere al adquirente del cupón la titularidad de un monedero bitcoin y una cuenta **BITRATE** (que se consigue descargándose su Aplicación personalizada) Al comprar un cupón el cliente adquiere una determinada cantidad de criptoactivos por una determinada cantidad de euros y a partir de ese momento puede decidir el momento en que activar o canjear

el cupón, momento en el que se produce la transferencia de bitcoins de los monederos de **BITRATE SA** al monedero del cliente.<sup>16</sup>

- VII) Estos Bitcoins adquiridos vía cupones y a los que se adicionaban los Bitcoins menados por la propia organización en la nave industrial de Alfajarín (Zaragoza) eran posteriormente convertidos en moneda Ethereum a través de casas de cambio online y presentados ante los clientes de **CRYPTOGOX** como réditos procedentes del funcionamiento del negocio fraudulento siendo ingresados en un principio en las direcciones facilitadas por los clientes de conformidad con lo estipulado en los contratos previamente configurados. Igualmente, estas cantidades blanqueadas a través del mecanismo expuesto *ut supra* eran usadas en parte para sufragar un lujoso tren de vida llevado por los acusados **ANTONIO, VITALY y JAVIER**.
- VIII) De las actuaciones realizadas durante la fase de instrucción ha quedado acreditado que **VITALY** operó el esquema de legitimación de capitales prevaleciendo de sus conocimientos como abogado especializado en materia mercantil y de gestión de productos de inversión, siendo él quien se encargaba de llevar a cabo las compras tanto de vehículos como de artículos de lujo una vez el dinero blanqueado era puesto a disposición de los acusados.

---

<sup>16</sup> Este novedoso mecanismo de blanqueo a través de cupones de criptomonedas adquiridas con dinero fiduciario y canjeables criptodivisas a la elección del tenedor está extraído de un caso real en el que un grupo criminal marroquí dedicado a la perpetración de estafas bancarias a través de técnicas de *phising* enviaba al extranjero las ganancias obtenidas en España a través de esta clase de operaciones habiendo blanqueado a través de cupones canjeables alrededor de 800.000 euros. Véase: SAP Madrid 704/2019 de 10 de octubre, FJ 3º (ECLI:ES: APM:2019:4990A)

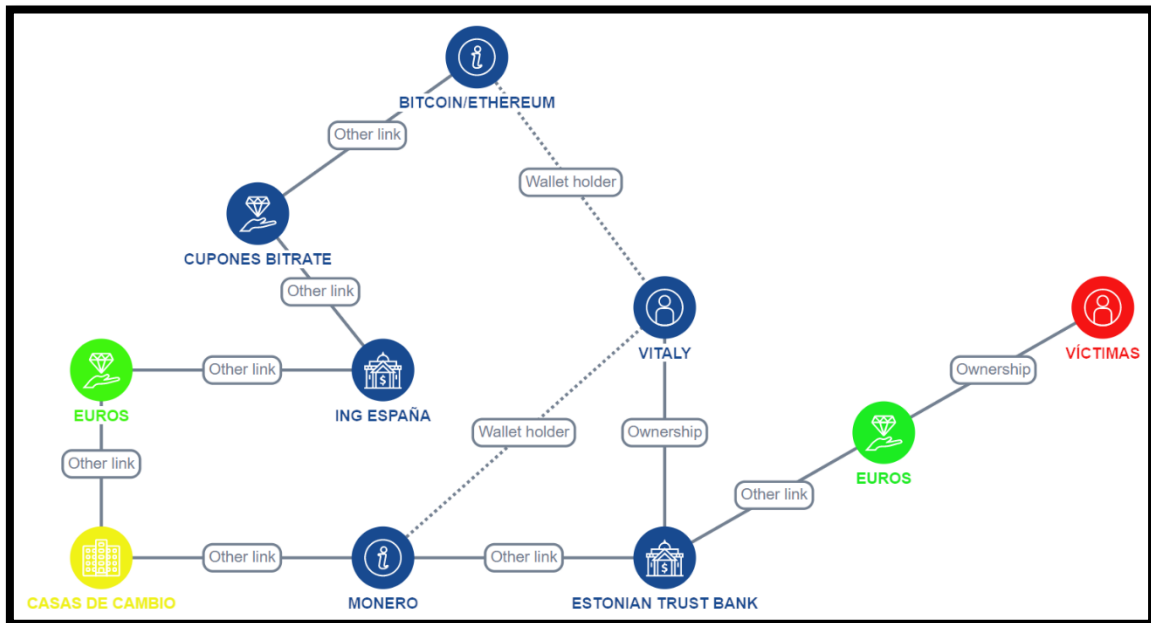


Diagrama elaborado por la Brigada Central de Delincuencia Económica y Fiscal reconstruyendo la trama de blanqueo de capitales gestionada por el acusado **VITALY**

Durante los 12 meses en que el entramado defraudatorio pivotante alrededor de **CRYPTOGOX** se mantuvo operativo se dieron determinadas circunstancias que pusieron de manifiesto si bien no el carácter criminal de la operativa liderada por la organización criminal integrada por **ANTONIO, VITALY** y **JAVIER** cuanto menos su carácter espurio. Así, en claro incumplimiento de las obligaciones establecidas por el art. 2.1 c) de la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo **CRYPTOGOX** no tenía instalado ningún tipo de control o sistema de *due diligence* mediante el cual dar cumplimiento a los requerimientos en materia de comprobación e información que la mencionada ley exige a las empresas de servicios de inversión. Por otro lado, con fecha de 15 de enero de 2022 la Comisión Nacional del Mercado de Valores (CNMV) publicó un aviso dando a conocer una serie de entidades mercantiles calificadas como no autorizadas o «*chiringuitos financieros*». Estas empresas se distinguían de acuerdo con el comunicado hecho público por la CNMV por operar en mercados altamente volátiles llevando a cabo servicios de inversión o de asesoramiento financiero sin contar con ningún tipo de autorización ni estar sujetas al marco regulatorio exigido en el sector.

Paralelamente, la CNMV publicó el mismo mes de enero una guía bajo el título Guía de Chiringuitos Financieros que mencionaba a **CRYPTOGOX** como una de estas entidades operantes en España y en la que exponía de forma pormenorizada las

principales técnicas que entramados como el liderado por los acusados **ANTONIO, VITALY** y **JAVIER** utilizan. Así, se hacía referencia expresa a las técnicas de referencias y recomendaciones personales en las que se basaba el funcionamiento de **CRYPTOGOX**, las apariencias de respetabilidad y éxito que concurren en el acusado **ANTONIO**, la oferta de grandes beneficios corriendo poco o ningún riesgo, el uso de un lenguaje muy complejo y de tecnicismos orientados a la ocultación del funcionamiento del negocio y la oferta de productos desconocidos o inexistentes.

Como quiera que el entramado defraudatorio estaba diseñado para la extracción de rentas y no para la gestión mercantil de un negocio que permitiera la generación de plusvalía llegó un momento en que, alrededor de la segunda semana de mayo del 2022, en el marco de la devaluación masiva de los criptoactivos que tuvo lugar a nivel internacional como consecuencia de la debacle de determinadas criptomonedas numerosos usuarios de la plataforma **CRYPTOGOX** comenzaron a solicitar la devolución de los fondos invertidos. De acuerdo con los contratos suscritos con la entidad el cliente no podía retirar la inversión inicial hasta pasados 2 años. No obstante, el cliente estaba autorizado a retirar las cantidades que con posterioridad invirtiera en la plataforma (de hecho, este era el aliciente para que la mayoría de las víctimas continuaran aportando rentas al esquema defraudatorio)

De este modo, al suceder que las noticias sobre la devaluación de las criptomonedas a nivel mundial alcanzaron amplia difusión en los medios de comunicación españoles a partir de la tercera semana de mayo las solicitudes de retirada de fondos de **CRYPTOGOX** alcanzaron a más del 60% de los clientes de la plataforma. Si bien en un principio los acusados **ANTONIO, VITALY** y **JAVIER** se plegaron a las solicitudes procediendo a hacer los reingresos reclamados para finales de mayo y debido al altísimo porcentaje de clientes que solicitaban devolución de sus fondos los acusados se negaron a acceder a tales pretensiones alegando que **CRYPTOGOX** procedería a congelar durante un tiempo indefinido las devoluciones a fin de evitar un riesgo de pérdida de liquidez. Esto generó no solo numerosas demandas en el ámbito de lo civil por incumplimiento de contrato sino además una importante pérdida de nuevos miembros, cuyo número fue languideciendo hasta el punto de no conseguir sumar ningún nuevo inversor al proyecto. Ante la súbita pérdida de lo que hasta entonces había venido siendo una corriente continua de víctimas que con sus aportaciones sufragaban la continuidad de

los pagos diarios el esquema defraudatorio se vio privado de un recurso fundamental con el que aceptar su *modus operandi*.

Ante esta situación, en un momento indeterminado de finales de junio los acusados **ANTONIO, VITALY y JAVIER**, actuando a través de **CRYPTOGOX**, cesaron unilateralmente de devengar las cuotas diarias sin realizar ningún tipo de notificación a los clientes. Paralelamente, los acusados bloquearon primeramente el acceso a la intranet de la página web de **CRYPTOGOX** destinada a los clientes para posteriormente interrumpir todo tipo de acceso a la misma a través de la desindexación de la dirección web de los servidores DNS. Igualmente, los acusados dejaron de responder tanto a las llamadas telefónicas como a los correos electrónicos que los clientes de **CRYPTOGOX** les dirigían a diario, procediendo a eliminar los perfiles de la plataforma de las redes sociales en las que ofrecían información sobre el modo de convertirse en inversor.

Debido a la situación a la que llegó en julio de 2022 (la plataforma en suspensión de pagos y los directivos de la mercantil **CRYPTO INVERSIÓN LIMITED** sin contestar a ninguna requisitoria de información por parte de los clientes y en paradero desconocido) un grupo de víctimas, asociados en una organización autodenominada Cryptogox Afectados, presentó querrela criminal contra los acusados **ANTONIO, VITALY y JAVIER** ante el Juzgado de Instrucción nº 15 de Madrid que ante la magnitud de los hechos se inhibió a favor del Juzgado nº 3 de la Audiencia Nacional alegando que conforme al art. 65. 1º c) de la Ley Orgánica del Poder Judicial los presentes hechos constituían una defraudación que podía llegar a afectar a un a generalidad de personas.

Como consta en autos, el Juzgado de Instrucción nº 3 de la Audiencia Nacional, dictó providencia en fecha de 3 de agosto en la que nombraba a la brigada Central de Delincuencia Económica y Fiscal bajo la dirección funcional de la Unidad Central de Delincuencia Económica y Fiscal (UDEP) del Cuerpo Nacional de Policía como única unidad actuante en el marco de las diligencias previas N° 000167/2022.

En el marco de las diligencias de investigación efectuadas por los agentes de la UDEF se puso en evidencia el carácter defraudatorio del entramado dirigido por los acusados **ANTONIO, VITALY y JAVIER**, así como la estructura de la organización criminal integrada por éstos. La dinámica de la actuación investigativa de los agentes de la UDEF hizo perentorio el recurso a medidas de investigación tecnológicas de las

reguladas en el Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, en concreto se solicitó a través de diligencia N° 1665/2022 al Juzgado de Instrucción N.º 3 de la Audiencia Nacional conforme a las disposiciones del art. 588ter LECRIM intervención de los dispositivos telefónicos propiedad de **ANTONIO** (con n° de teléfono 638194758), **VITALY** (con n° de teléfono 673817635) y **JAVIER** (n° de teléfono 684275917) Del análisis de las conversaciones interceptadas a raíz de la práctica de las mencionadas intervenciones se puso de manifiesto el carácter eminentemente criminal de las actuaciones de los acusados. Igualmente, con fecha 23 de febrero de 2022, a las 18:35 horas se produce una llamada de **ANTONIO** desde el número 638194758 al número 673817635 de **VITALY** produciéndose la siguiente conversación (Véase Documento N° 3 para transcripción completa):

*ANTONIO: Oye, necesito que me mandes cincuenta K (referencia a cincuenta mil euros) de Estonia (en referencia a la cuenta bancaria que la organización gestiona en Estonia) a Javier, que hay que ir comprando más servidores...*

*VITALY: ¿Pero ¿cómo, cincuenta K? ¿Y cómo quieres que lo haga?*

*A: Sí, sí. Cincuenta K. No sé cómo lo puedes hacer, pero Javier lo necesita ya porque me ha dicho que en Alfajarín están sacando mucha pasta con los ASICs y hay que aprovechar la oportunidad, que ahora el Bitcoin está por las nubes...*

*V: Ya, pero cincuenta es mucho ¿eh? No sé cómo lo voy a hacer*

*A: Pues tienes que moverte, pero ya. Ayer di una charla a casi trescientos tíos y han metido todos más de doscientos por cabeza. Y además me ha dicho Javier que tiene a uno de Madrid que le vende los ASIC súper baratos ¿No podrías utilizar las cuentas de ING?*

*V: Sí, supongo que sí que podría. Igual fraccionándolo todo en cantidades de menos de cinco mil podría hacer unas doce transferencias a Javier*

*A: Eso es, perfecto ¿tienes su número?*

*V: Sí, sí. No te preocupes. Que hablé con él la semana pasada y ya me dijo que me llamarías*

*A: Vale, pues quedamos en eso. Tú mándale cincuenta K y ya me apaño yo con él ¿va?*

*V: Venga va, no te preocupes. Nos vemos*

*A: Adiós*

Esta conversación pone de manifiesto la existencia de una organización criminal en la que cada uno de los acusados desempeñaba un rol muy bien definido. Así, mientras el acusado JAVIER ejercía el rol de captador de clientes y realizaba los actos necesarios para embaucarlos y conseguir las disposiciones de caudales, VITALY gestionaba la infraestructura ligada al blanqueo de los beneficios y JAVIER, por su parte, operaba la nave industrial y los procesadores ASIC mediante los fondos generados por la organización.

Igualmente, y con el fin de determinar el uso que de los servicios de la sociedad de información hacía el acusado **VITALY** en su rol de gestor del mecanismo de blanqueo de capitales de la organización de la que formaba parte se solicitó en diligencia N° 1715/2022 al Juzgado de Instrucción N.º 3 de la Audiencia Nacional registro telemático y a distancia de los dispositivos informáticos y electrónicos utilizados por el acusado. Así, la práctica de diligencias investigativas puso de manifiesto que **VITALY** se servía para realizar ingresos en las cuentas aperturadas en **ING ESPAÑA** de un mismo teléfono móvil modelo Samsung SM-G360F con N° IMEI 359149061490779 al que acoplaba diversas tarjetas SIM y con el que a través de plataformas de banca online dirigía los ingresos y desembolsos respecto a las mencionadas cuentas (Documento 4).<sup>17</sup>

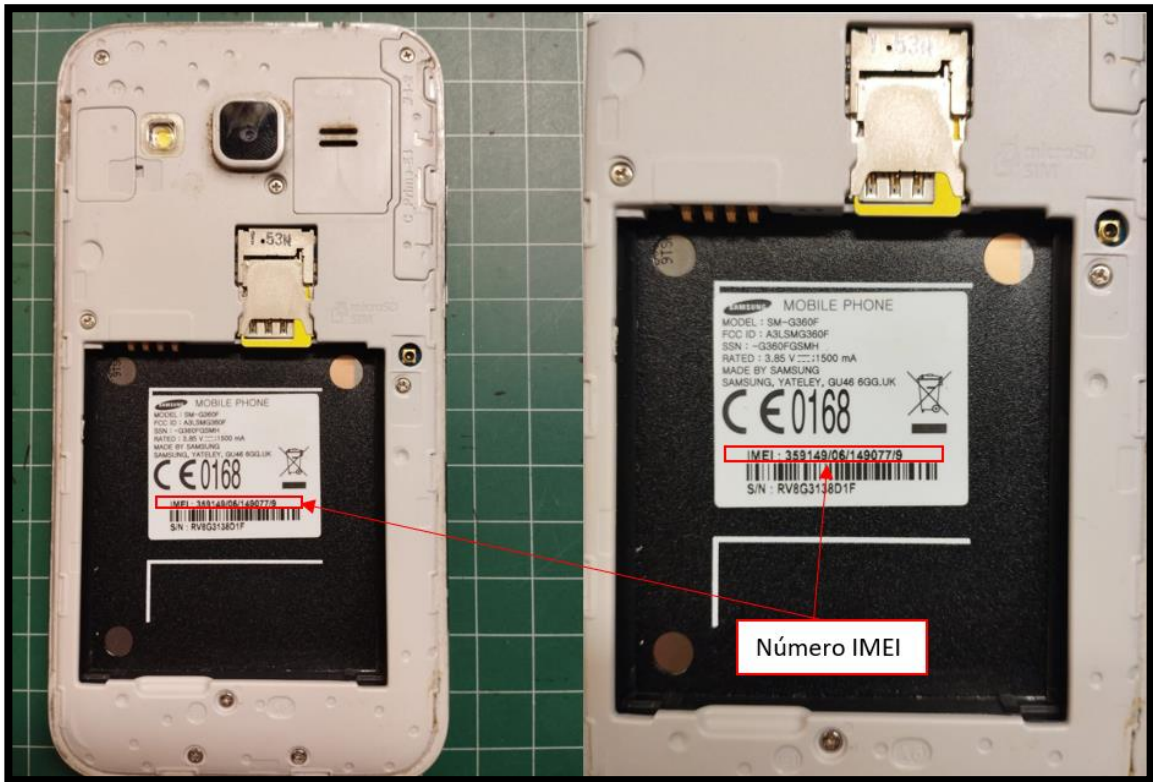
Igualmente, las pesquisas realizadas por los elementos adscritos a la Brigada Central de Delincuencia Económica y Fiscal permitieron descubrir que **VITALY** operaba las cuentas sitas en la entidad **ESTONIAN TRUST BANK** así como la conversión de moneda fiduciaria a criptomonedas y viceversa conectándose a internet a través de un ordenador portátil HP modelo EliteBook 850 G5 (hallado en poder del propio **VITALY** (a raíz de los registros practicados con posterioridad) identificado a través de la dirección MAC AC:B5:7D:8A:50:BF (Documento 5).<sup>18</sup>

---

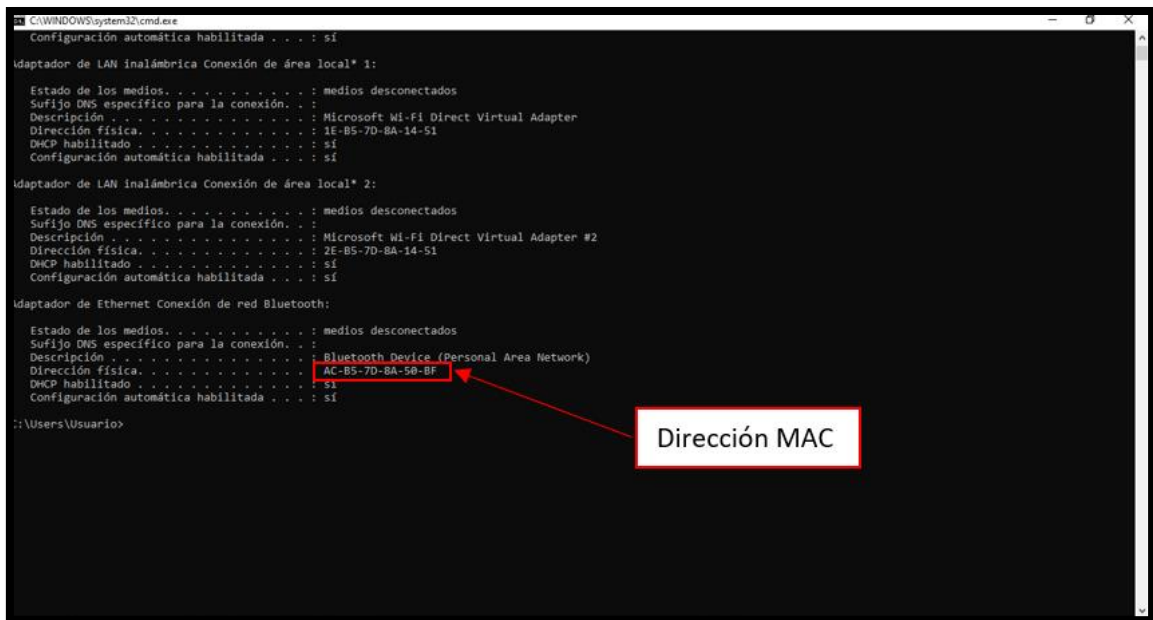
<sup>17</sup> El número IMEI (*International Mobile Equipment Identity*) es un código numérico que los fabricantes de telefonía móvil asocian con carácter exclusivo a cada teléfono móvil con el fin de designar unívocamente cada aparato. Está compuesto por quince dígitos. Los primeros seis (TAC o *Type Allocation Code*) designan al país en el que se comercializa, los dígitos séptimo y octavo (FAC o *Final Assembly Code*) designan al fabricante, los dígitos del noveno al catorceavo (SNR) designan el número de serie del teléfono y el último dígito cumple funciones de verificación. La ley de Enjuiciamiento Criminal, en su artículo 588 ter l) permite a la policía judicial «valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración [...] IMEI y [...] de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones».

<sup>18</sup> La dirección MAC (*Media Access Control*) o número MAC es un identificador alfanumérico utilizado para la identificación de la tarjeta de red o NIC (*Network Interface Card*), que es a su vez el adaptador de red que todo sistema informático utiliza para convertir los datos recibidos y transmitidos a través de la red





Documento 4. Teléfono móvil marca Samsung modelo SM-G360F con N° IMEI 359149061490779 hallado en poder de **VITALY**. El acusado se servía del dispositivo para recibir y enviar transacciones necesarias para el blanqueo de los fondos obtenidos. Obsérvese en rojo el número IMEI que permite la identificación unívoca del teléfono móvil.



Documento 5. Captura de pantalla realizada a través de un registro a distancia del ordenador portátil HP modelo EliteBook 850 G5 a través del cual el acusado **VITALY** efectuaba las transacciones necesarias

conforme a los protocolos correspondientes. La dirección MAC está compuesta por seis bytes, designando los tres primeros al fabricante y los otros tres a la propia tarjeta de red

para el blanqueo de los fondos obtenidos. Obsérvese en rojo la dirección MAC que permite la identificación unívoca de la tarjeta de red utilizada por el acusado para conectarse a Internet.

Asimismo, en el marco de la actividad investigadora realizada por los integrantes de la UDEF se hizo perentorio el registro de los domicilios de los acusados **ANTONIO** (sito en Calle Italia n° 25, 1° B), **VITALY** (sito en Calle Agustinos n° 52, 2° F) y **JAVIER** (sito en Calle los Sitios n° 21, 5° A) así como en la nave industrial del n° 30 del polígono industrial de Alfajarín (Zaragoza) Este registro fue solicitado por medio de diligencia n° 1678/2022 al Juzgado de Instrucción n° 3 de la Audiencia Nacional practicándose de forma simultánea el 15 de julio de 2022 a las 4:30 horas de la mañana por los agentes de los Grupos I y II de la Brigada Central de Delincuencia Económica y Financiera acompañados del Letrado de la Administración de Justicia del Juzgado Central de Instrucción n° 3 de la Audiencia Nacional en virtud de los correspondientes autos de entrada y registro.

Como resultado de los registros efectuados se intervinieron los siguientes efectos:

- Ocho ordenadores portátiles de marca HP modelo EliteBook 850 G5
- Cuatro teléfonos móviles marca Huawei modelo P636 8 GB
- Un teléfono móvil marca Samsung modelo SM-G360F con N° IMEI 342517627826352
- Veinticinco memorias USB Flash Kingston de treinta y dos GigaBytes de memoria
- Dos discos duros portátiles modelo Seagate Expansion Desktop 3.5 de capacidad de 16 TeraBytes
- Ciento cincuenta procesadores ASIC (*Application-Specific Integrated Circuit*) modelo Bitmain Antminer S19 Pro
- Cuatrocientos metros de cable trenzado tipo Ethernet UTP
- Cuatrocientos cincuenta disipadores de calor marca Intel con sus correspondientes ventiladores
- Herramientas y útiles diversos para posibilitar el puenteo de transformadores eléctricos
- Un enganche ilegal a la red eléctrica por medio de un cable de doble acometida
- Un monedero o *wallet fría* para Bitcoin y Monero en formato de tarjeta metálica con número de dirección asociada 45PBEairgR5JddGDorH1URSadrJx3J

- Un monedero o *wallet fría* activado por impresión biométrica de tipo dactilar de marca D´CENT con dirección Bitcoin 78PBEauekR3KddFEkeG3UEsfnrJx3I configurado para su activación mediante impresión dactilar del dedo índice derecho de **VITALY**
- Un monedero o wallet fría modelo Ledger Nano S Plus con dirección Ethereum 0x2b4k78ehj06h28391c89dc3909b9d81234ll9hab
- Una tarjeta de crédito de número 3847 7483 7195 8374 a nombre de **CRYPTO INVERSIÓN LIMITED** emitida por la entidad financiera **ESTONIAN TRUST BANK**
- Una tarjeta de crédito de número 2849 2839 3748 8391 emitida por la entidad ING vinculada a la Cuenta Nómina nº ES78 6475 5296 3659 6056 a nombre de **MARTÍN**
- Una tarjeta de crédito de número 2849 9304 1837 0349 emitida por la entidad ING vinculada a la cuenta Nómina ING nº ES37 8267 7295 8294 5920 a nombre de **GLORIA**
- Una tarjeta de crédito de número 9283 7495 9304 7154 emitida por la entidad ING vinculada a la cuenta Nómina ING nº ES92 7390 6185 2786 1896 a nombre de **SERGIO**
- Veinticinco mil euros en efectivo en billetes de distinto valor que se desglosan de la siguiente manera: treinta billetes de cincuenta euros, cuarenta billetes de doscientos euros y veinte billetes de cien euros
- Un coche modelo Mercedes Maybach (matrícula 3849-IER) a nombre de **VITALY**
- Un coche modelo Audi Q8 (matrícula 3940-EUR) a nombre de **VITALY**
- Un coche modelo Porsche Cayenne Turbo GT (matrícula 2839-HTA) a nombre de **VITALY**

De las pericias realizadas por los agentes de la UDEF encargados de la investigación se ha llegado a estimar que el monto total defraudado por la organización, calculado en función del número de afectados, así como de la cantidad estándar a invertir en la plataforma, oscilaría entre los veinticinco y los veintisiete millones de euros.



sujetos forman parte integrante de una agrupación de más de dos personas que de forma concertada y coordinada se reparten tareas y funciones con la finalidad de perpetrar ilícitos penales de conformidad con el tenor literal del tipo del art. 570 bis. Este carácter numérico ya ha sido resaltado por la jurisprudencia al exigirse «la unión de dos o más personas con la finalidad de cometer concretamente delitos para poder entender la intencionalidad delictiva conjunta, propia de las bandas».<sup>19</sup>

No obstante lo anterior, la principal particularidad de esta figura delictiva radica en la imprecisión de lo que ha de entenderse por organización criminal, especialmente de cara a su diferenciación respecto del grupo criminal regulado en el art. 570 ter. Así, conforme a la jurisprudencia del Tribunal Supremo es esencial el concepto de integración puesto que lo que se requiere de los sujetos activos es que se integren en una entidad «con un concierto y coordinación, o al menos aceptación y sumisión, que alcanza al establecimiento de las tareas o funciones encaminadas a la comisión de delitos. Cualquiera que sea la forma de integración [...] incluyendo como formas menos intensas la "participación activa", "formar parte" o la "cooperación" económica o de otra naturaleza».<sup>20</sup> Así pues, es obvio que en el caso que nos ocupa se da una participación activa de los tres acusados **ANTONIO, VITALY** y **JAVIER** quienes puestos de común acuerdo y coordinándose se reparte distintos roles (**ANTONIO** a cargo de la captación de víctimas y de conseguir la disposición de los fondos, **VITALY** encargado del blanqueo del producto del delito y **JAVIER** encargado de la reinversión de los beneficios y de mantener una apariencia de negocio operativo) cometen los hechos que se han mencionado. Por otro lado, es de destacar el ámbito internacional de sus operaciones, que si bien estaban basadas en la detracción de capitales en España opera una compleja trama de blanqueo de capitales en jurisdicciones tan lejanas como Estonia, Hong Kong o Singapur. No le faltaba razón al Tribunal Supremo al colegir que «la organización criminal [...] viene a ser la cara oculta de la globalización y que opera en diversos territorios con desconocimiento de las fronteras, teniendo intereses internacionales, y aprovechando en su caso las divergencias legislativas».<sup>21</sup>

---

<sup>19</sup> SAP de Madrid 505/2018 de 26 de junio (ECLI:ES:TS: 2019:3218) Si bien la sentencia se refiere a la banda latinoamericana de los Dominican Don't Play (DDP) utiliza el mencionado razonamiento para su tipificación como organización criminal a la luz del art. 570 bis

<sup>20</sup> STS 276/2021 de 25 de marzo, Fundamento Jurídico 3º (ECLI:ES:TS:2021:1308)

<sup>21</sup> STS 778/2010 de 29 de julio (ECLI:ES:TS: 2010:5114)

Abundando en la existencia del tipo penal del art. 570 bis, uno de los argumentos para distinguirlo del más amplio y benévolo precepto de grupo criminal del art. 570 ter es su tendencia a la estabilidad temporal puesta de manifiesto en el carácter prescindible de sus miembros. En este mismo sentido, la STS 1035/2013 de 9 de enero establece que para apreciar el tipo de organización criminal se exige que los autores hayan actuado «dentro de una estructura caracterizada por un centro de decisiones y diversos niveles jerárquicos, con posibilidades de sustitución de unos a otros mediante una red de reemplazos que asegura la supervivencia del proyecto criminal con cierta independencia de las personas integrantes de la organización, y que dificultan de manera extraordinaria la persecución de los delitos cometidos, aumentando al mismo tiempo el daño posible causado». <sup>22</sup> En este sentido, puede afirmarse que el papel de los acusados **ANTONIO, VITALY y JAVIER** encaja en los presentes modelos de conducta. En efecto, si bien el rol asumido por cada uno de ellos era característico de su particular proceder criminal no podemos sino concluir que precisamente esta compartimentalización funcional basada en la especialización delictiva convertía a cada uno de ellos en sujetos plenamente prescindibles superando de esta forma el mero concierto para delinquir basado en la oportunidad y aprovechamiento de la superioridad que la jurisprudencia ha venido en denominar codelincuencia. La propia STS 1035/2013 confirma este razonamiento al señalar que «lo decisivo es, precisamente, esta posibilidad de desarrollo del plan delictivo de manera independiente de las personas individuales, pues ello es lo que permite hablar de una empresa criminal».

En suma, la concurrencia del tipo de la organización criminal es asumida por la Sala Segunda del Tribunal Supremo en base a los criterios complementarios tanto de continuidad delictiva como de carácter prescindible de sus miembros tal y como se pone de manifiesto en la STS 356/2009 de 7 de abril al exigir la comisión del delito «mediante redes ya mínimamente estructuradas en cuanto que, por los medios de que disponen, por la posibilidad de desarrollar un plan delictivo con independencia de las vicisitudes que afecten individualmente a sus integrantes, su aprovechamiento supone una mayor facilidad para los autores, y

---

<sup>22</sup> STS 1035/2013 de 9 de enero, (ECLI:ES:TS:2014:220)

también una eventual gravedad de superior intensidad en el ataque al bien jurídico que se protege, debido especialmente a su capacidad de lesión».<sup>23</sup>

En cuanto a las cualidades de los acusados **ANTONIO, VITALY y JAVIER**, se concluye que no son simples sujetos activos del delito del art. 570 bis sino que además lo son en su condición de dirigentes puesto que fueron ellos quienes actuando con pleno conocimiento y voluntad procedieron a constituir, organizar, dirigir y coordinar la organización objeto de análisis en el presente escrito. Hemos de recordar que el tipo del art. 570 bis CP distingue entre dos figuras básicas: dirigentes y miembros o colaboradores. A los primeros se les asigna un rol primigenio y de liderazgo en tanto que a los segundos se les achaca tan solo la simple membresía así como determinados actos de colaboración o soporte (que puede ser de tipo material, humano o financiero) La Circular de Fiscalía 2/2011 de 12 de junio sobre la reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales dispone que «para calificar la conducta como de dirección, el sujeto deberá poseer en el marco de la organización, la responsabilidad efectiva y autónoma de adoptar decisiones que orientan la actuación de los miembros de la misma». En esta misma línea (precisamente recogida por la Circular 2/2011) el Tribunal Supremo afirma que tan solo puede asignarse un papel de promotor o directivo a quien «tenga encargada la responsabilidad de una función determinada y (...) desempeñe la correspondiente tarea de mando o decisión sobre otra u otras personas con las que en común tenga el cometido de planificar o ejecutar las correspondientes acciones, siempre dentro de la banda o grupo».<sup>24</sup>

De los anteriores razonamientos podemos deducir que los acusados **ANTONIO, VITALY y JAVIER** desempeñaban un rol directivo en el seno de la organización por ellos creada. En este sentido, **ANTONIO** planificaba y ejecutaba a su libre albedrío las operaciones de captación de víctimas, **VITALY** diseñaba los distintos mecanismos de blanqueo de las ganancias con autonomía y **JAVIER** disponía de independencia para la gestión del área o sección destinada

---

<sup>23</sup> STS 356/2009 de 7 de abril (ECLI:ES:TS: 2009:2074)

<sup>24</sup> STS 50/2007 de 19 de enero (ECLI: ES:TS: 2007:1025) Caso disolución en calidad de asociación ilícitas de las organizaciones *abertzales* JARRAI, HAIKA y SEGUI. El ámbito de la resolución incide en el espectro de las asociaciones pantalla de la organización terrorista ETA, si bien el contenido es plenamente predicable de los integrantes de organizaciones y grupos criminales.

a explotar la instalación eléctrica ilegal para nutrir la infraestructura de minado de criptomonedas sita en la nave industrial de Alfajarín

## **B) Del delito de estafa hiperagravada**

- II. Concorre en segundo lugar un delito continuado de estafa propia agravada del art. 74.2 y del artículo 250.2 CP en relación con el artículo 248 CP del que se reputan coautores conforme a los artículos 27 y 28 CP **ANTONIO, VITALY y JAVIER**.

La existencia de esta figura delictiva (regulada en la Sección 1ª del Capítulo II del Título XIII CP y atentatoria contra el patrimonio) exige un análisis particularmente detallado en la medida que la operativa criminal de los acusados orbita en todo momento alrededor de una finalidad lucrativa lograda merced al montaje y administración de un entramado defraudatorio dirigido a la extracción de rentas y del cual el resto de figuras delictivas evidenciadas en el presente escrito son accesorias y dependientes.

El delito de estafa tal y como queda definido en el artículo 248 CP señala que «cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno». De esta forma, queda patente que se trata de un delito plurisubjetivo de participación necesaria que requiere ante todo del elemento subjetivo del injusto que es el ánimo de lucro. En delitos como el presente; es decir, en delitos patrimoniales en los que los sujetos pasivos se ven afectados en cuanto a la disposición de elementos de su propiedad, es fundamental la distinción entre el simple perjuicio económico derivado de una gestión deficiente por parte del administrador o proveedor del bien/servicio y que puede o no ser abarcado por la voluntad del sujeto activo del despliegue de una conducta criminal dirigida por el ánimo de lucro. La distinción no es baladí en la medida que tal y como ha señalado DOPICO GÓMEZ ALLER «entre dolo de perjuicio patrimonial y ánimo de lucro existe una íntima relación, hasta el punto de que en algunos casos resulta arduo distinguirlos [...], residiendo el elemento distintivo entre dolo civil y estafa



[...] en el ánimo de lucro, entendido como ánimo de obtener un beneficio derivado directamente de la posesión del objeto».<sup>25</sup>

Es evidente que es el ánimo de lucro el que de forma lógica y racional guía la conducta de los acusados **ANTONIO, VITALY** y **JAVIER** puesto que tal y como establece la jurisprudencia de la Sala 2ª del Tribunal Supremo éste no es sino «cualquier ventaja, provecho, beneficio o utilidad que se proponga obtener el reo con su antijurídica conducta».<sup>26</sup> Conducta que dicho sea de paso «ha de inferirse [...] en función de los hechos anteriores, coetáneos y posteriores a los que son objeto de calificación penal».<sup>27</sup> De los hechos se deduce que los acusados operaron pues desde el primer momento con pleno ánimo de lucro, configurando un entramado societario al que proveyeron de medios humanos, técnicos y económicos dirigidos a otorgarle no solo credibilidad empresarial sino además capacidad operativa con la finalidad de conseguir captar grandes cantidades de dinero con el que adquirir bienes y servicios. El hecho que durante los registros practicados con fecha de 15 de julio de 2022 se hallasen elevadas cantidades de efectivo, numerosos aparatos tecnológicos adquiridos con los fondos obtenidos de los miembros de **CRYPTOGOX**, así como vehículos de motor de alta gama constituye prueba directa de que los acusados **ANTONIO, VITALY** y **JAVIER** actuaron en todo momento guiados por un evidente ánimo de lucro. En relación con lo anterior, se puede afirmar igualmente que los acusados actuaron de forma dolosa, con conocimiento y voluntad de estar perpetrando un delito de estafa<sup>28</sup>. Los elementos volitivos e intelectivos del dolo son, de conformidad con el tipo penal, concurrentes y consecuentes con las conductas típicas puesto que el «dolo característico de la estafa supone la representación por el sujeto activo, consciente de su maquinación engañosa, de las consecuencias de su conducta»<sup>29</sup>.

Siguiendo la tipificación del artículo 248 CP, el delito de estafa requiere de tres elementos concurrentes *sine qua non*. En primer lugar, se requiere del uso del engaño bastante como mecanismo embaucador para generar en el sujeto

---

<sup>25</sup> DOPICO GÓMEZ-ALLER, J. «Estafa y Dolo Civil: Criterios para su Delimitación», en *Dereito*, Vol. 21, nº1, 2012, p.21

<sup>26</sup> STS 416/2007 de 23 de mayo, FJ 12º (ECLI:ES:TS: 2007:3596)

<sup>27</sup> *Ibid*

<sup>28</sup> Sería posible incluso hablar en el caso que nos ocupa de un *Animus Nocendi*, es decir, de un ánimo de engañar y/o perjudicar, si bien se trata de un concepto más propio de la jurisdicción civil aplicable en el marco de incumplimientos contractuales y el fraude de ley

<sup>29</sup> STS, 507/2003 de 9 de abril, FJ 2º (ECLI:ES:TS:2003:2509)

pasivo el error de apreciación como segundo elemento típico. Error que llevará a la víctima al tercer requisito, la disposición patrimonial en perjuicio de su propia persona o de otra a él vinculada.

La Sala 2ª del Tribunal Supremo se ha pronunciado reiteradas veces sobre el concepto de engaño exigido por el tipo del art. 248 CP. Así, el Tribunal Supremo ha hablado de una doble vertiente del engaño; exigiendo en primer lugar que «el engaño ha de ser idóneo, de forma que ha de tenerse en cuenta tanto su capacidad objetiva para hacer que el sujeto pasivo del mismo, como hombre medio, incurra en un error, como, al mismo tiempo, las circunstancias subjetivas del sujeto pasivo, o dicho de otra forma, su capacidad concreta para resistirse al artificio organizado por el autor». Por otro lado, se exige en segundo lugar «una relación de causalidad entre el engaño que provoca el error y el desplazamiento patrimonial que da lugar al perjuicio, de donde se obtiene que aquél ha de ser precedente o, al menos, concurrente, al momento en que tal desplazamiento se origina».<sup>30</sup> Abundando en este concepto, la STS 895/2003 de 19 de junio llegaba a calificar la exigencia de engaño bastante como un tópico «doctrinal y jurisprudencial». Esta resolución exigía para apreciar el engaño bastante el ponderar «la suficiencia de la simulación de verdad para inducir a error, a tenor del uso social vigente en el campo de actividad en el que aconteció la conducta objeto de examen y considerando la personalidad del que se dice engañado».<sup>31</sup> Es decir, no se trata de cualquier ardid ilusorio que tenga por objeto embaucar al sujeto pasivo, sino que ha de tratarse de un engaño definido por el Código Penal como bastante y por la jurisprudencia como idóneo en el sentido que debe tener tal entidad que entre este primer elemento de la estafa y el segundo (el error) llegue a establecerse un nexo causal en tanto que sin el primero no se daría el siguiente.

En conclusión, la apreciación de este primer elemento típico se basa en un análisis del caso concreto que ha de llevar a deducir la existencia de error bastante que «no deja de ser un estado de consciencia o elemento psicológico que deberá objetivarse mediante el examen concreto de las circunstancias que rodean al negocio jurídico que justifica el desplazamiento, y que revelen más allá de la mera suposición o probabilidad la certeza de que cuando se perfeccionó el sujeto activo

---

<sup>30</sup> STS 839/2012 de 23 de octubre, FJ 3º (ECLI:ES:TS:2012:7161)

<sup>31</sup> STS 895/2003, de 18 de junio, FJ Único (ECLI:ES:TS:2003:4242)

no tenía intención alguna en cumplir con las obligaciones derivadas del mismo».<sup>32</sup> Así las cosas, es innegable que en el presente caso los acusados **ANTONIO, VITALY** y **JAVIER** utilizaron engaño bastante para generar en sus víctimas el error que las condujo a realizar las aportaciones patrimoniales. Así, **ANTONIO** se valió de su condición de empresario reconocido y del prestigio público que ello le suponía para producir en las víctimas la falsa certeza de estar depositando sus fondos en manos de un administrador fiable y responsable, **VITALY** utilizó los previamente analizados canales financieros para conseguir hacer circular los fondos y hacer creer a las víctimas mediante ingresos del todo artificiales que **CRYPTOGOX** funcionaba realmente y **JAVIER**, gracias a su actividad de mantenimiento de servidores en la nave industrial de Aljafarín, hizo pensar a los usuarios de la red que estaban invirtiendo en un negocio real y plenamente operativo. Es de destacar que las aportaciones de los tres acusados no constituyen compartimentos estancos en los cuales encorsetar las conductas típicas de éstos, por el contrario, los respectivos comportamientos de **ANTONIO, VITALY** y **JAVIER** en cada una de sus especificidades delictivas están completamente entrelazados en tanto que cada uno de ellos es imprescindible para los demás. Así, sin mantenimiento de servidores ficticios por **JAVIER** no habría podido **ANTONIO** embaucar a las víctimas, siendo las sumas de dinero manejadas por **VITALY** la forma última de hacer creer a aquéllas a través de los pagos iniciales que **CRYPTOGOX** era una empresa viable.

En cuanto al segundo elemento típico de la estafa se refiere, el error, queda probado que también concurre en el presente caso. Así, en palabras de ANTON ONECA el error puede definirse como «una representación mental que no se corresponde con la realidad» provocado en el sujeto pasivo por medio del engaño analizado previamente que le conduce a llevar a cabo una disposición patrimonial que de otro modo no hubiera realizado pues su juicio se encuentra contaminado ante una situación que se le presenta diáfana cuando en realidad está alterada y/o deformada por voluntad del sujeto activo. No obstante, no se trata de cualquier error. No basta con que el sujeto pasivo tenga simples dudas o dilemas a la hora de realizar o no la disposición patrimonial (a fin de cuentas, nos encontramos en un campo puramente económico-patrimonial en el que el nivel conocimiento de

---

<sup>32</sup> SAP de Las Palmas (Sección 1ª) 307/2017 de 13 de octubre, FJ 6º (ECLI:ES:APGC:2017:1783)

la realidad pocas veces casa con las actuaciones de los sujetos a la hora de invertir o realizar unos u otros actos dispositionales) sino que el error que le ha sido inducido ha de ser esencial.<sup>33</sup> El Tribunal Supremo ha exigido precisamente este error esencial en un sujeto pasivo que siendo «desconocedor o con conocimiento deformado o inexacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio del agente [...] llega a actuar bajo una falsa presuposición, a emitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se produce el traspaso patrimonial».<sup>34</sup> Abundando en el error producido en los sujetos pasivos del caso que nos ocupa (los miles de víctimas del esquema defraudatorio operado a través de **CRYPTOGOX**), no puede afirmarse que se tratara de clientes de una empresa de servicios de inversión sujeta a las contingencias de un mercado extremadamente agresivo y volátil como lo es el de las criptomonedas que se vieran perjudicadas en sus intereses por las circunstancias de la realidad económica. Como ya ha establecido el Tribunal Supremo en relación con los delitos defraudatorios, «el deber de autoprotección predicable de toda persona» que al realizar una inversión asume el riesgo de perderla «no puede desplazar indebidamente sobre los perjudicados la responsabilidad de comportamientos en que la intención de engañar es manifiesta».<sup>35</sup> En el caso de **CRYPTOGOX** se aprecia una situación fáctica en la que los acusados **ANTONIO, VITALY** y **JAVIER** proceden a través de conductas concertadas y coordinadas a embaucar a una pluralidad de personas, la mayoría de ellas jóvenes o en edad de jubilación y sin experiencia en materia de inversiones financieras, sin existir ningún tipo de respaldo real en relación con las operaciones de gestión de *masternodos* publicitadas como la verdadera fuente de ingresos de la plataforma **CRYPTOGOX**. Queda patente pues la existencia del engaño examinado *supra* como elemento desencadenante de un error esencial en los miles de víctimas del esquema defraudatorio gestionado por **ANTONIO, VITALY** y **JAVIER**, error que en ningún caso puede calificarse de suficientemente «burdo, grosero o esperpéntico» como para excluir «el mecanismo

---

<sup>33</sup> BALMACEDA-HOYOS, G. citando a ANTÓN ONECA, «El Delito de Estafa: una Necesaria Normativización de sus Elementos Típicos», en *Revista Estudios Socio-Jurídicos*, Vol. 13, núm. 2, julio-diciembre de 2011, p. 190

<sup>34</sup> STS 353/2000 de 1 de enero, FJ 3º (ECLI:ES:TS:2000:1615)

<sup>35</sup> STS 371/2015 de 17 de junio, FJ 3º (ECLI:ES:TS:2015:2758)

para producir error en otro».<sup>36</sup> En efecto, en el contexto actual de los mercados de criptomonedas nada de burdo hay en el error de la víctima que se ve embaucada y realiza una inversión en un supuesto sistema de minado de criptomonedas que pese a lo enrevesado de su funcionamiento es idéntico a miles de sistemas semejantes perfectamente legales y en funcionamiento.

Como consecuencia del nexo causal existente entre el engaño bastante generado por **ANTONIO, VITALY** y **JAVIER** y el error esencial producido en los sujetos pasivos hace aparición el tercer elemento integrante de la estafa; la disposición patrimonial perjudicante, que «puede consistir en cualquier acción del engañado que causa un perjuicio patrimonial propio o de tercero, entendiéndose por tal la entrega de una cosa como la prestación de un servicio por el que no se obtiene la contraprestación».<sup>37</sup> En efecto, en el marco del presente asunto se puso de manifiesto como miles de personas embaucadas por **ANTONIO, VITALY** y **JAVIER** llevaron a cabo numerosísimas transferencias de tipo electrónico y bancario dirigidas a la cuenta bancaria EE90 5412 3455 7384 5905 aperturada por **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK** y operada por aquéllos. Si bien en un primer momento, con el fin de mantener las apariencias y crear una falsa sensación de funcionalidad, los acusados llevaron a cabo los reintegros prometidos a un número indeterminado de clientes éstos se sufragaban no con la explotación de *masternodos* dado que estos eran inexistentes, sino a costa de las inversiones de nuevas víctimas. Es pues innegable la existencia de un claro perjuicio económico con respecto a las personas que invirtieron cantidades en el sistema **CRYPTOGOX**.

Una vez probada la existencia del tipo de estafa en cuanto a los elementos básicos exigidos por el artículo 248 CP, debe abundarse llegado este punto en la entidad de la conducta de los acusados **ANTONIO, VITALY** y **JAVIER** puesto que ésta constituye un supuesto hiperagravado del tipo penal denominado en el argot de la criminalidad financiero-patrimonial como «estafa piramidal».

En el universo de los tipos penales de la Sección 1ª del Capítulo VI del Título XIII del Código Penal, las estafas piramidales juegan un papel vital como el máximo exponente de la conducta defraudatoria tanto por número de afectados como, fundamentalmente, por la cantidad de capitales que son susceptibles de

---

<sup>36</sup> Ibid

<sup>37</sup> STS 132/2007 de 16 de febrero (ECLI:ES:TS: 2007:1931)

captar. Las estafas piramidales han sido definidas por el Tribunal Supremo como aquellas en las que «el autor se dedica a captar capital prometiendo la realización de importantes inversiones por medio de alguna entidad mercantil previamente constituida que sirve de señuelo. Se promete a los posibles clientes el abono de sustanciosos intereses, sin que después existan los negocios que habrían de producir los ingresos que permitirían devolver el capital y los intereses convenidos. Lo habitual es que en una primera etapa se abonen a los primeros inversores el capital y los intereses valiéndose de las aportaciones de los sucesivos clientes. En estas conductas delictivas "piramidales o en cascada" los sujetos realizan una puesta en escena en ejecución de un designio criminal único encaminada a defraudar a un número indeterminado de personas, pudiendo proyectarse esta acción defraudatoria sobre una persona que a su vez convenza a otras, como consecuencia de su propio engaño, a realizar similares inversiones. Este modelo piramidal de estafa conduce necesariamente a la frustración del negocio prometido, pues en la medida en que se incrementa el capital recibido, aumentan exponencialmente las necesidades de nuevos ingresos para abonar los intereses, hasta que el actor deja de pagarlos y se apropia definitivamente de los capitales fraudulentamente recibidos».<sup>38</sup>

Como puede apreciarse en el presente caso concurren todos los elementos típicos configuradores de la estafa piramidal. En primer lugar, los acusados, sirviéndose de la mercantil **CRYPTO INVERSIÓN LIMITED** como vehículo societario y utilizando la plataforma **CRYPTOGOXX** como señuelo, captan a una pluralidad de pequeños y medianos inversores prometiéndoles a éstos altísimas rentabilidades a cambio de unas operaciones negociales del todo inexistentes. En segundo lugar, se produce el sostenimiento del esquema defraudatorio con base en las aportaciones realizadas por los nuevos socios, cuyas inversiones son utilizadas para sufragar los intereses debidos a los socios iniciales generando un sistema basado en la retroalimentación que se perpetúa en el tiempo ligándose su supervivencia a la capacidad de los acusados **ANTONIO, VITALY** y **JAVIER** de seguir captando nuevas víctimas. Finalmente se produce la debacle del sistema dada la insuficiencia los capitales que se van ingresando de cara al pago de los

---

<sup>38</sup> STS 900/2014 de 26 de diciembre, FJ 3ª (ECLI: ES: TS: 2014: 5573)

intereses debidos teniendo lugar la apropiación definitiva de todo el montante captado por el esquema defraudatorio por los acusados, quienes cortan toda comunicación con los inversores y les privan de acceso a toda información relativa al funcionamiento de **CRYPTOGOX**.

Ahora bien, una cosa es calificar los presentes hechos como integrantes del prototípico supuesto de la estafa piramidal y otra muy distinta el incardinarlos en un artículo específico del Código Penal. Así las cosas, los acusados **ANTONIO, VITALY** y **JAVIER** incurrir en la modalidad continuada de estafa agravada del artículo 250.2 del Código Penal al exceder el monto de lo defraudado de los 250.000 euros exigidos por el tipo, llegando a totalizar según las pericias efectuadas en el marco de la instrucción del presente procedimiento un montante total de alrededor de veintisiete millones de euros.

El conflicto que ha planteado a los tribunales la combinación de la modalidad de estafa agravada y la continuidad delictiva ha generado una abundantísima jurisprudencia del Tribunal Supremo que ha definido claramente la aplicación de uno u otro criterio en función del tipo de estafa ante el que el juzgador se encuentre. En este sentido, hay que recordar que de acuerdo con la sección 1ª del Capítulo VI del Título XIII existen cuatro modalidades básicas de estafa. La primera por debajo de los 400 euros está tipificada como delito leve por el art. 249; la segunda entre los 400 y los 50.000 euros según la aplicación de un criterio interpretativo de los artículo 249 y 250.1.5º está penada con prisión de seis meses a tres años y constituye el tipo básico; la tercera entre los 50.000 y los 250.000 euros está prevista en el art. 250.1.5º y está penada con prisión de uno a seis años y multa de seis a doce meses y finalmente la cuarta (la modalidad hiperagravada) está prevista en el artículo 250.2 y penada con prisión de cuatro a ocho años y multa de doce a veinticuatro meses.<sup>39</sup> Pues bien, la apreciación de la circunstancia hiper agravada del artículo 250.2 concurre en el supuesto que nos ocupa dado que los acusados procedieron a defraudar un montante (alrededor de veintisiete millones de euros) que excede en mucho de la cuantía prevista por el tipo (250.000 euros<sup>40</sup>) teniendo en cuenta que en el supuesto típico de la estafa «el

---

<sup>39</sup> Téngase en cuenta que la modificación operada en el tipo de la estafa por la LO 14/2022 ha cambiado la distribución numérica de los artículos, si bien la estructura sigue siendo en esencia la misma.

<sup>40</sup> Para la confirmación de la aplicación de la modalidad hiper agravada de estafa del art. 250.2 por superar los 250.000 euros *vid* SAP Santander 105/2021 de 30 de abril FJ 4º (ECLI:ES: APS:2021:167) El caso versaba sobre una persona estafada en España por otra que le requería de forma continuada numerosas

valor de lo defraudado se identifica con el del desplazamiento patrimonial causado por el acto de disposición ejecutado por el error derivado del engaño».<sup>41</sup>

Este delito concurre además en la modalidad continuada específica de los delitos patrimoniales denominado por la doctrina y la jurisprudencia como «delito masa» y que el Código Penal tipifica en su artículo 74.2 como una modalidad de delito continuado en el que la pena a imponer no se calcula según las reglas del artículo 74.1 (la pena correspondiente a la infracción más grave en su mitad superior) sino con relación al perjuicio total causado. Las características del delito masa han sido definidas por la jurisprudencia como «una modalidad agravada del delito continuado, pero que tiene características propias que le dotan de una autonomía y sustantividad propias» en base a dos criterios significativos:<sup>42</sup>

- a) Un dolo únicamente «preconcebido» frente al dolo del delito continuado, que puede ser tanto «preconcebido como ocasional»<sup>43</sup>
- b) La «notoria gravedad» que no deja de ser «lo notorio unido al sustantivo gravedad, en clave económica» y «múltiples perjudicados»<sup>44</sup>

La mencionada Audiencia Provincial de Murcia concluía que por delito masa había de entenderse aquel «plan preconcebido» que «contempla ya desde el inicio el dirigir la acción contra una pluralidad indeterminada de personas, sin ningún lazo o vínculo entre ellas, y de cuyo perjuicio individual pretenden obtener los sujetos activos, por acumulación, un beneficio económico muy superior».<sup>45</sup>

SAINZ CANTERO, por su parte, haciendo énfasis tanto en las características de esta figura delictiva como en su naturaleza jurisprudencial define el delito masa como «un ente jurídico o realidad natural con vida propia, que deriva de una realidad dolosa dirigida certeramente al logro de un fraude o

---

sumas de dinero para poder llevar a cabo operaciones quirúrgicas del todo inexistentes en Rumanía y mediante las que se extrajo a la víctima un total de 922.000 euros durante dos años. La Audiencia Provincial aprecia tanto una modalidad continuada como la existencia del subtipo hiper agravado del art. 250.2 por superar el monto de lo defraudado ampliamente los 250.000 euros

<sup>41</sup> STS 166/2013 de 8 de marzo FJ 5º (ECLI:ES:TS: 2013:1110)

<sup>42</sup> SAP Murcia 125/2014 de 22 de abril FJ 5º (ECLI:ES: APMU: 2014:955)

<sup>43</sup> Ibid

<sup>44</sup> Ibid

<sup>45</sup> Ibid



perjuicio colectivo de sujetos indeterminados plurales, que se captan a priori en la intención delictiva, planificada, del autor».<sup>46</sup>

Ha de recordarse, por otro lado, que el delito masa se configura como la modalidad patrimonial del delito continuado, que conforme al artículo 74.1 del Código Penal consiste en la ejecución por parte del sujeto activo de una pluralidad de acciones u omisiones en ejecución de un plan preconcebido o aprovechando idéntica ocasión y mediante las cuales vulnera preceptos penales de igual o semejante naturaleza viéndose penada la conducta con la pena más grave en su mitad superior pudiendo llegar hasta la mitad inferior de la pena superior en grado.

Así pues, puede afirmarse que en el caso que nos ocupa se verifica la modalidad del delito masa en tanto que los acusados proceden a ejecutar a lo largo del tiempo un plan para estafar a un amplio colectivo de víctimas llevando a cabo de manera reiterada y durante un espectro amplísimo de tiempo que llega a abarcar el año de duración una multiplicidad de actos consistentes en la captación de numerosas cantidades de dinero que les son enviadas de buena fe por las víctimas del esquema defraudatorio. No obstante lo anterior, la cuestión de la posible aplicación de la modalidad continuada del artículo 74.1 al presente caso merece un razonamiento particular en tanto que la doctrina y jurisprudencia mayoritaria se oponen a la misma.

Ha de analizarse llegado este punto la posibilidad de aplicar la modalidad del delito masa del artículo 74.2 a un delito de estafa aplicándose igualmente la prescripción del artículo 74.1. Ciertamente es que el Tribunal Supremo se ha pronunciado sobre la compatibilidad entre el delito masa del art. 74.2 y la aplicación de la pena en su mitad superior contenida en el art. 74.1. Así, en la sentencia 173/2013 de 28 de febrero remarcaba el Tribunal que «no existe razón alguna de política criminal que justifique la sustracción del delito continuado de naturaleza patrimonial respecto de la regla agravatoria prevista en el art. 74.1 del CP. De ahí la importancia del acuerdo adoptado en el mencionado Pleno, con arreglo al cual, el delito continuado de naturaleza patrimonial también habrá de

---

<sup>46</sup> SAINZ CANTERO, J.A., «El Delito Masa», en *Anuario de Derecho Penal y Ciencias Penales*, Fascículo 3, 1971, p. 659

ser sancionado mediante la imposición de la pena, determinada con arreglo al perjuicio total causado, en su mitad superior. Ello no es sino consecuencia de aplicar al delito patrimonial las razones de política criminal que justifican la norma del art. 74.1 del CP».<sup>47</sup>

No obstante, lo anterior, el Tribunal también ha negado la doble aplicación de las reglas penológicas del art. 74.1 y 74.2 CP en relación con aquellos casos en que «su aplicación [la del art. 74.1] fuere contraria a la prohibición de doble valoración».<sup>48</sup> Así, en palabras de la Sala Segunda se trataría de garantizar «la exclusión del efecto agravatorio en determinados supuestos, para impedir que su aplicación conduzca a la doble incriminación de un mismo hecho. Así, por ejemplo, en las ocasiones en que la suma del perjuicio total ocasionado se tome en consideración para aplicar el subtipo agravado de especial gravedad atendiendo al valor de la defraudación, resultaría redundante aplicar además el efecto agravatorio de la regla primera del art. 74 del CP. Se trata de evitar la aplicación de la regla general agravatoria, prevista en el art. 74.1 del CP, a aquellos delitos en los que el importe total del perjuicio ha determinado ya un cambio de calificación jurídica y la correlativa agravación, es decir a delitos de estafa o apropiación indebida que, por razón de su importe total, se desplazan del tipo básico al subtipo agravado».<sup>49</sup>

Como se puede comprobar, es esto lo que precisamente sucede en el presente caso. Los acusados **ANTONIO, VITALY** y **JAVIER** pergeñan un esquema defraudatorio diseñado para lograr disposiciones patrimoniales de mayor o menor cuantía que si bien habrían de ser superiores a los 100 euros (la cuota mínima requerida para invertir en el esquema **CRYPTOGOX**) en ningún caso superaron los 250.000 euros individualmente consideradas, abundando las aportaciones entre la horquilla de los 100 y los 2.000 euros. Por ello, no podría aplicarse en el presente caso la circunstancia penológica prevista para el delito continuado en el art. 74.1 puesto que la cuantía de 250.000 euros ya ha sido

---

<sup>47</sup> STS 173/2013 de 28 de febrero FJ 7º (ECLI:ES:TS: 2013:921)

<sup>48</sup> Acuerdo No Jurisdiccional de la Sala 2ª del Tribunal Supremo de 18 de julio de 2007 relativo a la unificación de criterios en torno a la penalidad del delito continuado de estafa y apropiación indebida. El tenor literal del acuerdo establece que *“el delito continuado siempre se sanciona con la mitad superior de la pena. Cuando se trata de delitos patrimoniales la pena básica no se determina en atención a la infracción más grave, sino al perjuicio total causado. La regla primera del art. 74.1 queda sin efecto cuando su aplicación fuera contraria a la prohibición de doble valoración”*

<sup>49</sup> Ibid.

prevista para apreciar la modalidad hiper agravada del art. 250.2 CP. De lo contrario, es decir, en caso de apreciar el ser la estafa superior a los 250.000 euros tanto para aplicar la modalidad de estafa hiper agravada del art. 250.2 CP como para aplicar la regla penológica del art. 74.1 CP, se estaría incurriendo en palabras del Tribunal Supremo en «vulneración de la prohibición constitucional de non bis in idem».<sup>50</sup>

En conclusión, en el presente caso se imputa a los acusados **ANTONIO**, **VITALY** y **JAVIER** la comisión en calidad de coautores conforme a los artículos 27 y 28 CP de un delito continuado en su modalidad de delito masa del art. 74.2 de estafa hiper agravada del artículo 250.2 CP en relación con el artículo 248 CP en cuanto a la conducta típica se refiere.

### C) Del delito de blanqueo de capitales

- III. Concorre en tercer lugar un delito de blanqueo de capitales del artículo 301.1 CP del que responderían criminalmente en concepto de coautores conforme a los artículos 27 y 28 CP los acusados **ANTONIO** y **VITALY** siendo paralelamente de aplicación las circunstancias del art. 305.5 CP en cuanto al decomiso de toda eventual ganancia obtenida por éstos, así como del art. 303 CP en cuanto a la imposición de una pena de inhabilitación especial para profesión empresa, industria o comercio al acusado **ANTONIO** por perpetrar el delito prevaleándose de su condición de empresario.

Nos encontramos ante el que posiblemente sea uno de los delitos más subjetivos que pueda hallarse en la actual legislación penal. Así, GARCÍA NORIEGA ha definido el delito de blanqueo de capitales como una serie de «operaciones por las que los activos generados por actividades ilícitas [...] son reintroducidos en el sistema económico aparentando un origen lícito», llegando a hablar técnicamente no ya de simple blanqueo sino de «legitimación de capitales» o «legitimación de activos».<sup>51</sup> Se trata en suma de una conducta que tiene por finalidad un ánimo de distracción que recoge el artículo 301.1 CP al definir el blanqueo en su tipo básico como la adquisición, posesión, utilización, conversión o transmisión de bienes a sabiendas de «que éstos tienen su origen en una actividad

---

<sup>50</sup> Ibid.

<sup>51</sup> GARCÍA NORIEGA, A., «Blanqueo y Anti-Blanqueo de Capitales» en *Como se Lava el Dinero y Cómo se Combate el Lavado*, Difusión Jurídica, 2010, p. 15

delictiva, cometida por él [el autor] o por cualquiera tercera persona. O realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos», tal y como estipula el Código Penal. Se trata pues de un delito común (en la medida que no requiere especiales cualidades del sujeto activo), de propia mano y mixto alternativo, atentatorio con respecto a la licitud «el orden socioeconómico, y dentro de este, los intereses concretos susceptibles de ser tutelados materialmente por el sistema punitivo. Entre otros, el interés del Estado en controlar el flujo de capitales procedentes de actividades delictivas ejecutadas a gran escala y que pueden menoscabar el sistema económico, afectando también al buen funcionamiento del mercado y de los mecanismos financieros y bursátiles». <sup>52</sup> En cuanto a la finalidad de los autores del delito de blanqueo de capitales, la jurisprudencia ha establecido de modo reiterado que el tipo del artículo 301 CP tiene por finalidad «evitar que los autores de un delito logren incorporar al tráfico económico legal los bienes, dinero, ganancias o beneficios procedentes de sus actividades ilícitas, e impedir que puedan disfrutar de lo así obtenido si logran otorgarle apariencia de licitud, haciendo jurídicamente inatacable su relación con dicho patrimonio». <sup>53</sup>

En los delitos patrimoniales (y dentro de ellos particularmente los cometidos a través de instrumentos tecnológicos) no es difícil demostrar que los sujetos activos persiguen una finalidad lucrativa. No obstante, no sucede lo mismo con la prueba del origen de los efectos receptados o blanqueados, puesto que tal y como ha señalado el Tribunal Supremo «el blanqueo de capitales no es un delito de sospecha: exige como cualquier otro, prueba de la concurrencia de todos y cada uno de sus elementos típicos, entre los que se encuentra el origen criminal (y no meramente ilícito, ilegal o antijurídico) de los bienes». <sup>54</sup>

Así, en el presente caso es perentorio demostrar en primer lugar que los acusados eran conocedores de la naturaleza ilícita de los fondos, algo que es sencillo en lo que a **ANTONIO** respecta, pero no tanto a **VITALY** (que se limitaba a hacer circular el dinero entre cuentas) ni a **JAVIER** (que tenía como

---

<sup>52</sup> STS 677/2019, de 23 de enero FJ 4º (ECLI:ES:TS:2020:148)

<sup>53</sup> Sentencia de la Sala de lo Penal de la Audiencia Nacional 35/2019 de 20 de diciembre (ECLI:ES:AN:2019:4716)

<sup>54</sup> STS 677/2019, de 23 de enero FJ 4º (ECLI:ES:TS:2020:148)

función mantener en funcionamiento la instalación de minado de Alfajarín). En segundo lugar es necesario acreditar que las cuantías de dinero obtenidas por los acusados **ANTONIO**, **VITALY** y **JAVIER** fueron objeto de un tratamiento destinado a garantizar la ocultación del origen ilícito de los mismos de cara a insertar esta conducta en el tipo del art. 301.1 CP.

En lo que respecta al primer punto y en relación con **ANTONIO**, no puede sino afirmarse el carácter directivo que el acusado desempeña en el marco del esquema defraudatorio. Así pues, fue **ANTONIO** quien diseñó el sistema societario a través del cual se cometió la estafa y era igualmente él quien decidía el destino de las rentas extraídas a las víctimas, todo lo cual permite afirmar su carácter preponderante y decisivo para el funcionamiento tanto de la organización criminal como de los mecanismos delictivos a través de ésta operados.

En lo que a **VITALY** respecta, tampoco debería haber duda de su responsabilidad penal en concepto de coautor, puesto que es él mismo quien prevaliéndose de su condición de abogado mercantil y por lo tanto de sus conocimientos especializados desempeña el rol de «blanqueador» en la organización criminal integrada por los tres acusados siendo pues quien concibe, opera y garantiza el mantenimiento en el tiempo de la operativa criminal ligada al aprovechamiento y legitimación de las sumas de dinero mal habidas. Esto mismo afirmaba el Tribunal Supremo en su sentencia 974/2012 de 5 de diciembre al afirmar la autoría con respecto al delito de blanqueo de capitales de un abogado que desempeñaba un papel semejante puesto que su conducta «no puede ser calificada de acto neutral, al no limitarse a una labor de asesoramiento profesional. La especial estructura de las sociedades constituidas [...] y la opacidad de las transmisiones [...] gestionando y administrando sus cuentas con las que adquirirían los inmuebles, hacia esta especialmente idónea para el blanqueo de dinero de origen ilícito y la comisión de los delitos [...]».<sup>55</sup>

---

<sup>55</sup> STS 974/2012 de 5 de diciembre FJ 8º (ECLI:ES:TS: 2012:8701) Esta sentencia analizaba entre muchas otras conductas el papel desempeñado por un abogado que diseñó y regentó desde España un sistema societario radicado en jurisdicción de nula tributación [paraísos fiscales] a través del cual ofrecía servicios de inversión inmobiliaria a múltiples organizaciones criminales dedicadas al tráfico de drogas. El Tribunal aduce que la gestión de semejante organigrama societario no podía incardinarse en las denominadas «acciones neutrales» [actos de simple gestión que excluirían la tipicidad de la conducta] sino por su utilidad para la ocultación de la naturaleza delictiva de los capitales objeto de inversión eran plenamente subsumibles en el tipo del art. 301.1 CP.

Este mismo razonamiento, aplicado al caso que nos ocupa y salvando el hecho de que la organización integrada por **ANTONIO, VITALY** y **JAVIER** no disponía de una red societaria internacional a través de la cual llevar a cabo el blanqueo de las ganancias obtenidas, permite afirmar una conducta idéntica por parte de **VITALY**.

Con relación a **JAVIER**, es necesario recalcar que su participación en la operativa ligada al blanqueo de capitales se limitaba a aportar a la organización determinadas cantidades de Bitcoins obtenidas a través del minado artesanal que él mismo gestionaba en la nave arrendada por la organización en la localidad de Alfajarín y que eran utilizadas para aparentar la solvencia de **CRYPTOGOX** ante los clientes así como a hacer uso de los capitales blanqueados para adquirir productos y servicios y, en suma, disfrutar de las ganancias generadas por la operativa criminal de la que formaba parte. Así las cosas, no cabe imputar al mencionado **JAVIER** la comisión del delito de blanqueo de capitales en tanto que su conducta consistente en el minado de Bitcoins ya ha sido tenida en cuenta para afirmar su participación en el delito de estafa en tanto que el hecho de disfrutar de los productos del delito blanqueados por los acusados **ANTONIO** y **VITALY** no supone de por sí una conducta típica del delito de blanqueo. Así, la sentencia 265/2015 de 29 de abril disponía al analizar la posible coexistencia entre un delito de tráfico de drogas (art. 368 CP) y uno de blanqueo de capitales (art. 301.1 CP) que «aunque el ánimo de disfrute de las ganancias no constituya un requisito típico del delito de tráfico de drogas, la obtención de beneficio y ganancias con el mismo, y su ulterior disfrute, integran un binomio de difícil escisión, de modo que la imposición de una pena autónoma por el mero hecho de adquirir, poseer o utilizar las ganancias obtenidas podría infringir la prohibición de doble incriminación».<sup>56</sup> A la luz de lo expuesto, si el Ministerio Fiscal decidiera imputar al acusado **JAVIER** la participación en el delito de blanqueo de capitales por

---

<sup>56</sup> STS 265/2015 de 29 de abril FJ 9º (ECLI:ES:TS: 2015:1925) Esta resolución reviste especial interés en tanto que desgrana en profundidad la punibilidad del denominado «auto blanqueo», es decir, el blanqueo de las ganancias por el autor del delito del que aquéllas proceden. En concreto, la sentencia analiza la conducta de la integrante de una asociación delictiva dedicada a coordinar redes de correos de droga que contrabandeaban pequeñas cantidades de cocaína entre República Dominicana y España. La recurrente aducía que el disfrute de los bienes procedentes de los delitos cometidos (fundamentalmente a través de la adquisición de vehículos) no suponía una conducta típica de blanqueo. Sin embargo, el Tribunal Supremo reiteró la pena por el delito de blanqueo afirmando que el hecho de que la recurrente hubiera puesto los vehículos adquiridos con el producto del tráfico de drogas a nombre de diversos familiares suponía el uso de éstos como «testaferros» yendo pues la conducta más allá del simple disfrute de los vehículos al certificarse un evidente ánimo de ocultación del origen delictivo de los fondos.

haber aportado parte de las criptomonedas que se mezclaban con los productos de la estafa en la que él participaba en calidad de coautor se estaría infringiendo el principio de *ne bis in idem* informador de nuestro ordenamiento jurídico. Por otro lado, y en relación con el simple disfrute del producto del delito en la mencionada sentencia 265/2015 el Tribunal Supremo afirmaba que «es necesario precisar que la acción típica sancionada como delito de blanqueo no consiste en el simple hecho de adquirir, poseer o utilizar los beneficios adquiridos sino, como precisa el tipo, en realizar estos u otros actos cuando tiendan a ocultar o encubrir el origen ilícito de las ganancias».<sup>57</sup>

Hemos de centrarnos llegado este punto en analizar hasta qué punto las acciones realizadas por el acusado VITALY tenían por objeto disimular el origen delictivo del dinero reconvertido en criptomonedas, puesto que tal y como ha señalado el Tribunal Supremo «la esencia del tipo [de blanqueo de capitales] es, por tanto, la expresión “con la finalidad de ocultar o encubrir el origen ilícito” [...] finalidad u objeto de la conducta que debe encontrarse presente en todos los comportamientos descritos por el tipo».<sup>58</sup>

Recordemos que éste acusado, utilizando la cuenta EE90 5412 3455 7384 5905 aperturada a nombre de **CRYPTO INVERSIÓN LIMITED** en la entidad financiera **ESTONIAN TRUST BANK** llevaba a cabo la compra de criptoactivos Monero (XMR) a través de casas de cambio localizadas en Hong Kong y Singapur. Las diligencias de investigación llevadas a cabo durante la fase de instrucción por parte de la Brigada Central de Delincuencia Económica y Financiera de la UDEF Central de la Comisaría General de Policía General del Cuerpo Nacional de Policía pusieron de manifiesto que esta práctica tenía lugar a través del ordenador portátil HP modelo EliteBook 850 G5 identificado a través de la dirección MAC AC:B5:7D:8A:50:BF (hallado en poder del propio **VITALY**) Así, durante el lapso de tiempo a lo largo del cual la organización criminal integrada por los acusados **ANTONIO, VITALY** y **JAVIER** se mantuvo operativa fueron incesantes las operaciones realizadas a través del mencionado ordenador portátil.

Estas operaciones seguían la siguiente dinámica: VITALY, accediendo a la cuenta EE90 5412 3455 7384 5905 del **ESTONIAN TRUST BANK** a través

---

<sup>57</sup> Ibid

<sup>58</sup> Ibid

de la plataforma de banca online facilitada por la entidad a sus clientes realizaba múltiples transacciones a las cuentas bancarias titularidad de diversas casas de cambio ubicadas en Hong Kong y Singapur con la finalidad de adquirir la criptodivisa denominada Monero (XMR) que quedaban alojadas en un monedero o *wallet fría* para Bitcoin y Monero en formato de tarjeta metálica con número de dirección asociada 45PBEairgR5JddGDorH1URSadrJx3J (hallado en poder de VITALY durante el registro de la nave arrendada por la organización en la localidad de Alfajarín el 15 de julio de 2022)

Posteriormente **VITALY** procedía a enajenar las criptodivisas Monero (XMR) utilizando las mismas casas de cambio obteniendo a cambio una determinada cantidad de dinero fiduciario (normalmente euros) que podía conllevar o no ganancias en función de las fluctuaciones del mercado y del tiempo transcurrido entre la compra y la venta. **VITALY** instruía a las casas de cambio con las que interactuaba a fin de que los euros intercambiados por criptomoneda Monero (XMR) fueran transferidos a las tres cuentas abiertas por él en **ING ESPAÑA** utilizando fotocopias de DNI ajenos.

Llegado este punto, y utilizando a una pluralidad de personas que no llegado a ser identificadas **VITALY** conseguía extraer numerosas cantidades de euros de las mencionadas cuentas aperturadas en **ING ESPAÑA** dotándoles de tarjetas de crédito asociadas a aquéllas instruyéndoles para obtener cantidades que nunca excedieran de los 500 euros a fin de no activar ningún protocolo AML<sup>59</sup> implementado por la entidad.<sup>60</sup>

---

<sup>59</sup> Un protocolo AML (*Anti Money Laundering Protocol* o *Protocolo Anti Blanqueo de Capitales*) es un mecanismo utilizado por las entidades financieras y demás operadores del ámbito bancario y comercial con el fin de detectar patrones de conducta incardinables en técnicas de blanqueo que permitan la activación de *red flags* o *banderas rojas*, es decir, alertas del sistema que bloquean la operación o proceden a abrir un parte de incidencias para obtener mayor información. Normalmente los protocolos AML se gestionan a través de complejos programas informáticos diseñados para el filtrado de millones de transferencias u operaciones financieras

<sup>60</sup> En cuanto al comportamiento de estos sujetos, si bien queda fuera del objeto de análisis considero necesario señalar que constituye una de las modalidades de blanqueo que llevan a cabo quienes han sido denominado tanto en el ámbito policial como judicial como «mulas» o «muleros», definidos por la Audiencia Provincial de Madrid como terceras personas (...) que (...) suelen ser captados mediante correos electrónicos también masivos e indiscriminados, en los que se les realiza una supuesta oferta laboral con la promesa de obtener una alta retribución económica, exigiéndoles a cambio la apertura de una cuenta bancaria, la recepción en ella de distintas transferencias de personas desconocidas y, finalmente, la remisión inmediata de dichas cantidades a terceras personas, también desconocidas, empleando para ello los sistemas de envío de dinero antes mencionados, previa detracción de una comisión porcentual de los ingresos. Vid. SAP 166/2020 de 2 de junio, FJ 3º (ECLI:ES: APM:2020:4742)



Con este dinero las mencionadas personas se dirigían (siempre instruidas por el acusado **VITALY**) a determinados comercios en los que procedían a la adquisición de cupones **BITRATE**. Para la adquisición de estos cupones, las personas instruidas por el acusado **VITALY** aportaban la dirección Bitcoin 78PBEauekR3KddFEkeG3UESfnrJx3I, vinculada un monedero o *wallet fría* activado por impresión biométrica de tipo dactilar de marca D´CENT con configurado para su activación mediante impresión dactilar del dedo índice derecho de **VITALY** y que fue hallado en su poder con ocasión del registro practicado en Alfajarín el 15 de julio de 2022. En esta dirección se alojaban igualmente los Bitcoins minados por la organización en la nave gestionada en la mencionada localidad, como demuestra el hecho de que los procesadores ASIC hallados durante el registro del 15 de julio de 2022 estuvieran configurados para derivar las criptomonedas obtenidas a la misma dirección Bitcoin.

Posteriormente, el acusado **VITALY** llevaba a cabo la conversión de los Bitcoins en moneda Ethereum merced a operaciones de conversión en las mismas casas de cambio utilizadas durante las primeras fases del tracto de blanqueo siendo esta última criptomoneda la utilizada para realizar los pagos a los clientes de **CRYPTOGOX**, así como para la adquisición de bienes y productos de lujo que los acusados **ANTONIO**, **VITALY** y **JAVIER** disfrutaban personalmente. Prueba de esto último son los tres vehículos [un Mercedes Maybach (matrícula 3849-IER), un Audi Q8 (matrícula 3940-EUR) y un Porsche Cayenne Turbo GT (matrícula 2839-HTA) todos ellos a nombre de **VITALY** habiéndose demostrado en sede de instrucción que fueron adquiridos por el mencionado acusado a través de transferencias realizadas desde las cuentas aperturadas en **ING ESPAÑA**.

Tras el análisis de los comportamientos llevados a cabo por el acusado **VITALY** y por las personas que actuaban bajo su dirección cabe concluir que, efectivamente, la operativa financiera de los hechos que nos ocupan tenía por finalidad la ocultación del origen delictivo de los fondos obtenidos y disfrutados por los tres acusados.

Ello se deduce en primer lugar del tipo de bien (criptomonedas) utilizado por la organización criminal integrada por los acusados no solo a la hora de cometer la estafa que nos ocupa sino a lo largo del tracto de blanqueo concebido y operado por **VITALY**. Es necesario remarcar que la elección de las

criptomonedas Bitcoin, Monero (XMR) y Ethereum no ha sido en este caso meramente casual. Si en este caso se ha optado por utilizar estos bienes como mecanismos de inversión y conversión de riqueza ha sido precisamente por el tipo de facilidades que otorgan de cara a la perpetración de delitos y al disfrute de sus réditos. La Oficina de las Drogas y el Delito de las Naciones Unidas (UNODC) ha señalado el uso de las monedas virtuales y por extensión de las criptomonedas como «instrumentalizadoras del delito»<sup>61</sup> en base a criterios tales como la rapidez e irreversibilidad de las transacciones, la conversión de dinero fiduciario a formato virtual y viceversa, la facilidad para la conversión de un tipo de moneda virtual a otra, el diseño encaminado a facilitar el anonimato, lo ilimitado de las transacciones y patrones de transferencia deliberadamente ofuscados.<sup>62</sup>

En cuanto a la naturaleza de las criptomonedas en si mismas, el hecho de que sean un activo inmaterial y por lo tanto intangible no impide clasificarlas como un bien. Si bien la regulación en materia de criptomonedas es de por si escasa y la jurisprudencia prácticamente inexistente hemos de recordar la sentencia 326/2019 en la que el Tribunal Supremo señalaba que «el bitcoin no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin».<sup>63</sup> *Ceteris paribus*, semejante razonamiento sobre el Bitcoin permite una concepción idéntica del resto de criptomonedas en tanto que su funcionamiento es notablemente similar, por no decir idéntico. Ha sido precisamente la naturaleza fungible de las criptomonedas una de las razones que han inducido al legislador a modificar recientemente el Código Penal incluyendo la denominación de «instrumentos de pago distintos al efectivo» para contemplar la posibilidad del uso de medios de pago distintos del dinero fiduciario para llevar a cabo conductas delictivas. Esta definición se encuentra contenida en el artículo 399 ter por el que se describen los instrumentos de pago distintos del efectivo

---

<sup>61</sup> UNITED NATIONS OFFICE ON DRUGS AND CRIME, «*Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*», junio 2014, p. 27. Disponible [online] en: <file:///C:/Users/Usuario/Desktop/Crypto%20ML/Money%20Laundering/Manual%20UNODC%20Monedas%20virtuales.pdf> (Fecha de consulta: 28 de noviembre de 2022)

<sup>62</sup> *Ibid*

<sup>63</sup> STS 326/2019 de 20 de junio, FJ 3º (ECLI:ES:TS:2019:2109)

como «cualquier dispositivo, objeto o registro protegido, material o inmaterial, o una combinación de estos, exceptuada la moneda de curso legal, que, por sí solo o en combinación con un procedimiento o conjunto de procedimientos, permite al titular o usuario transferir dinero o valor monetario incluso a través de medios digitales de intercambio».<sup>64</sup>

La relativa novedad del uso de criptomonedas como método de blanqueo de capitales es pues la causa de la escasísima jurisprudencia al respecto, lo que no obsta a que determinadas resoluciones judiciales hayan ido arrojando luz sobre un área tan opaca como la que nos ocupa. Así, el Auto 619/2022 de la Audiencia Nacional tipificaba el uso que una organización criminal hacía de plataformas de intercambio o *exchange* online de criptomonedas para canalizar las ganancias procedentes de la explotación de emisiones televisivas ilegales vía servidores web ubicados en el extranjero como blanqueo de capitales del art. 301 CP.<sup>65</sup> En la misma línea, el Auto 241/2021 de 30 de junio de la Audiencia Nacional tipificaba como blanqueo de capitales la conducta de un ciudadano sueco afincado en España que se dedicaba a «recibir, almacenar y transacciones de efectivo y criptomonedas [...] en grupo y en gran escala, ocultándoselas a terceros y sabiendo que procedían de delitos».<sup>66</sup>

---

<sup>64</sup> Tal y como expone el preámbulo de la LO 14/2022 de 22 de diciembre la introducción del art. 399 ter en el Código Penal trae causa de las exigencias de la Directiva 2019/713 de 17 de abril que «otorga especial relevancia a los medios de pago inmateriales, y entre ellos, los soportes digitales de intercambio». De hecho, el legislador llega a afirmar que por soporte digital de intercambio ha de entenderse «aquellos que permiten efectuar transferencias de dinero electrónico, de monedas virtuales y otros criptoactivos, ahora bien, en estos dos últimos casos, solo en la medida en que puedan usarse de manera habitual para efectuar pagos. Por ello, es palmario que el ámbito de protección que ofrece esta reforma se extiende a las monedas de carácter virtual». Dicho sea de paso, el legislador ha admitido la inclusión en semejante término de las monedas virtuales y criptoactivos, cubriéndose en cierto modo las espaldas con la coartada de la rápida evolución tecnológica al afirmar que «quedan incluidos, por tanto, todos los instrumentos de pago distintos del efectivo, incluidas las monedas virtuales y otros criptoactivos que se utilicen como medio de pago y los monederos electrónicos en una definición lo suficientemente abierta como para permitir la flexibilidad necesaria para adecuarse a los rápidos avances tecnológicos».

<sup>65</sup> Auto 619/2022 de 3 de noviembre de la Sección 4ª de la Sala de lo Penal de la Audiencia Nacional (ECLI:ES:AN: 2022:9718A) La resolución analiza la operativa de parte de la organización criminal liderada por un ciudadano iraní afincado en España dedicada a la distribución «pirata» de señal de televisión que en menos de dos años generó alrededor de 15 millones de euros merced a una red internacional de unos dos millones de clientes. En palabras del propio tribunal los acusados se servían de «transferencias internacionales a otras sociedades, creaban cuentas en plataformas de banca online y realizaban transferencias en cantidades que no levantasen sospechas, y cuando ya no podían hacer uso de estas vías acudían a métodos paralelos como el Sarraf, que es un sistema de compensación basado en la confianza para envío de dinero a otro país a cambio de una comisión eludiendo el control bancario».

<sup>66</sup> Auto 241/2021 de 30 de junio de la Sección 3ª de la Sala de lo Penal de la Audiencia Nacional, FJ Único (ECLI:ES:AN:2021: 5372A) La resolución analiza la procedencia de una Orden Europea de Detención y Entrega (mecanismo jurídico que ha venido a sustituir a la extradición pasiva en el ámbito de la Unión Europea y que se encuentra regulada en el Título II de la Ley 23/2014 de 20 de noviembre de Reconocimiento Mutuo de Resoluciones Penales en el Ámbito de la Unión Europea) por la que Suecia

Vemos pues que el conocimiento del origen ilícito de los fondos blanqueados es requisito *sine qua non* para apreciar el tipo del artículo 301.1 CP. El Tribunal Supremo ha establecido incluso una regla taxativa en cuanto a esto se refiere al afirmar que «para acreditar que el recurrente tenía conocimiento de la procedencia delictiva del dinero que blanqueaba, han de tomarse en consideración cuatro factores: en primer lugar, y en lo que se refiere a la precisión de las actuaciones delictivas, nuestra doctrina jurisprudencial no exige el conocimiento de los detalles o pormenores de las operaciones específicas de tráfico de las que procede el dinero, sino exclusivamente el conocimiento de su procedencia genérica de dicha actividad. En segundo lugar, y en lo que se refiere a la naturaleza del conocimiento [...] el conocimiento exigible no implica saber (en sentido fuerte), como sucede cuando el conocimiento se deriva de la observación científica de un fenómeno, o de la implicación personal y directa del sujeto como protagonista de la actividad de tráfico (lo que solo tendría lugar en casos de auto blanqueo), sino que se trata de un conocimiento práctico, del que se obtiene a través de la experiencia y de la razón, y que permite representarse una conclusión como la más probable en una situación dada [...] En tercer lugar, y como consecuencia de lo anterior, en lo que se refiere al dolo exigible, basta con el eventual, siendo suficiente que el acusado disponga de datos suficientes para poder inferir que el dinero procede del tráfico de estupefacientes, y le resulte indiferente dicha procedencia [...] Y, en cuarto lugar, en cuanto a la prueba, nuestra doctrina afirma que basta con la indiciaria, que es la que ordinariamente nos permitirá obtener una conclusión razonable sobre el conocimiento interno del sujeto». <sup>67</sup>

Semejantes conclusiones predicen un conocimiento del origen delictivo de los activos blanqueados no ya directo sino al que se puede incluso llegar vía deducciones o conclusiones a la luz de los indicios disponibles y la experiencia del sujeto activo y no pueden sino llevarnos a afirmar sin el menor ápice de duda que las operaciones realizadas por el acusado **VITALY** demuestran a todas luces que éste sabía del origen delictivo del dinero que convertía en criptomonedas. Esto

---

solicitaba a España la extradición de un ciudadano sueco afincado en España que desde la ciudad de Uppsala recibió, almacenó y transfirió 53 millones de coronas suecas (alrededor de 4.750.000 euros al cambio actual) en forma de criptomonedas y dinero en efectivo procedente muy seguramente del tráfico de drogas  
<sup>67</sup> STS 149/2017 de 9 de marzo, FJ 18º (ECLI:ES:TS:2017:847)

puede afirmarse en tanto que las diligencias de investigación practicadas por los agentes de la Brigada Central de Delincuencia Económica y Fiscal ponen de manifiesto la confabulación directa entre **ANTONIO** y el propio **VITALY** de cara a la recepción de unos fondos obtenidos en base al engaño utilizado para cometer el delito de estafa examinado *ut supra*, algo que ha quedado patente que era de conocimiento del segundo. Así, tal y como se indica en los Fundamentos de Hecho del presente escrito, con fecha 23 de febrero de 2022, a las 18:35 horas, se produce una llamada de **ANTONIO** desde el número 638194758 al número 673817635 de **VITALY** en la que el primero requiere al segundo que le envíe 50.000 euros desde la cuenta gestionada en el **ESTONIAN TRUST BANK** a una de las cuentas que la organización tenía aperturadas en **ING ESPAÑA** ya que acababa de dar «una charla a casi trescientos tíos y han metido todos más de doscientos por cabeza». Es pues obvio que el acusado **VITALY** conocía el hecho de que el dinero que continuamente convertía en criptomonedas que dificultaban sobremanera el eventual rastreo de los fondos tenía su origen en una estafa perpetrada en coalición con los acusados **ANTONIO** y **JAVIER**.

Y sin embargo, el hecho de que el artículo 302.1 CP contemple una agravación del delito de blanqueo de capitales por pertenencia a organización criminal nos lleva a subsumir el mencionado tipo penal en un concurso de leyes con el delito de pertenencia a organización del artículo 570 bis CP a resolver conforme a la regla de la alternatividad del artículo 8.4 CP tal y como prevé el artículo 570 quáter 2 CP al estipular que «en todo caso, cuando las conductas previstas en dichos artículos [en referencia a los delitos reguladores de la organización y grupo criminales] estuvieren comprendidas en otro precepto de este Código, será de aplicación lo dispuesto en la regla 4.<sup>a</sup> del artículo 8».

En este sentido se pronuncia la Circular de la Fiscalía General del Estado nº 2/2011 sobre la reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales al señalar que «en consecuencia, en los supuestos en que se plantee un conflicto de normas entre los arts. 515.1 y 570 bis CP, los Sres. Fiscales aplicarán el criterio de alternatividad previsto en el art.

8.4 CP, de conformidad con lo establecido en el art. 570 quáter CP, de modo que deberán aplicar el tipo con pena más grave, esto es, el art. 570 bis». <sup>68</sup>

En la misma línea, la circular establece que «si bien, la regla prevista en el art. 8.4 tiene carácter subsidiario respecto del resto de los criterios establecidos en el art. 8 para la resolución de los conflictos de normas, sin embargo, su aplicación directa ha de prevalecer por decisión del legislador expresada en el citado art. 570 quáter 2 in fine, opción justificada desde el planteamiento de que el mayor desvalor del hecho determina la aplicación de la pena más grave para evitar sanciones atenuadas incongruentes por la existencia de discordancias punitivas entre los distintos tipos penales [...]».

Ha de tenerse en cuenta llegado este punto que, pese al carácter aparentemente doctrinal ofrecido por la circular 2/2011 ésta no deja de ofrecer criterios meramente orientativos. En puridad, es necesario reconocer el variadísimo trato dado por la jurisprudencia a casos en los que, como sucede con el que nos ocupa, concurre un delito de organización criminal con un delito específicamente agravado por pertenencia a organización criminal. Así, MARÍN DE ESPINOSA afirma que la solución más adecuada pasa por apreciar «un concurso de delitos (real o ideal) entre el tipo básico correspondiente - sin la agravación de pertenencia a organización- y algunos de los delitos de asociación, organización o grupo criminal»<sup>69</sup>. La ya mencionada Circular 2/2011 afirma tal posibilidad al estipular «los Sres. Fiscales cuidarán de aplicar, de acuerdo con lo dispuesto en el art. 570 quater CP, conforme al criterio de alternatividad, un concurso de delitos entre el art. 570 bis o el art. 570 ter, en su caso, y el tipo correspondiente al delito específicamente cometido con todas sus circunstancias si bien prescindiendo de la agravación específica de organización, cuando la pena así aplicada sea superior a la que prevé el subtipo agravado».

Es pues de rigor imputar a los acusados **ANTONIO** y **VITALY** la comisión de un delito de blanqueo de capitales del artículo 301.1 CP con

---

<sup>68</sup> En este caso la circular 2/2011 se refiere al concurso de leyes entre el delito de asociación ilícita del art 515 CP y el de organización criminal del artículo 570 bis. No obstante, el ejemplo puede ser extrapolado a todos aquellos tipos penales que conlleven agravaciones por pertenencia a organización criminal

<sup>69</sup> MARÍN DE ESPINOSA CEBALLOS, E., «La Responsabilidad Criminal de los Miembros de una Organización o de un Grupo Criminal (arts. 570 bis y 570 ter CP): ¿un Problema de Autoría y Participación o de Tipicidad?» en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 24-25, 2022, pp. 1-32

aplicación de la disposición del artículo 301.5 y del art. 303 en lo que al decomiso de las ganancias y a la pena de inhabilitación profesional se refieren.

#### **D) Del delito de falsedad documental**

- IV. Concorre en cuarto lugar un delito de falsedad de documento privado del artículo 395 CP en relación con el artículo 290.1. 1º y 2º CP del que respondería en concepto de autor conforme a los artículos 27 y 28 CP el acusado **VITALY**.

Recordemos que con relación a este tipo penal la conducta del acusado consistió en la obtención de fotocopias de los Documentos Nacionales de Identidad de los ciudadanos españoles **MARTÍN, GLORIA y SERGIO** procediendo la alteración de las fotografías incluidas en los originales para utilizarlos junto a tres correos electrónicos creados al efecto aperturar tres cuentas bancarias en la entidad **ING ESPAÑA** con el fin de recibir las ganancias previamente blanqueadas en el marco del tracto de legitimización concebido por el propio **VITALY**.

El Tribunal Supremo ha tenido previamente la oportunidad de analizar la conducta consistente en la alteración de una fotocopia de un documento oficial como es el DNI enmarcándolo dentro de la conducta propia de la falsificación de documento privado. Así, en la sentencia 11/2015 de 29 de enero afirmaba el Tribunal Supremo que «las fotocopias de documentos son sin duda documentos en cuanto escritos que reflejan una idea que plasma en el documento original, si bien la naturaleza oficial del documento original no se transmite a la fotocopia, salvo en el caso de que la misma fuese autenticada (...) Por ello una falsedad, en cuanto alteración de la verdad del documento, realizada sobre una fotocopia no autenticada de un documento oficial, público o mercantil, no puede homologarse analógicamente a la falsedad de un documento de la naturaleza que tenga el original, por lo que sólo podrá considerarse como una falsedad en un documento privado».<sup>70</sup>

Este Ministerio Fiscal se pliega pues al anterior razonamiento. En la medida que las falsedades materiales de los artículos 390.1. 1º y 2º suponen en el

---

<sup>70</sup> STS 11/2015 de 29 de enero, FJ 6º (ECLI:ES:TS:2015:393)

caso que nos ocupa la alteración no ya de una copia autenticada sino de una simple fotocopia de un documento público y oficial como es el Documento Nacional de Identidad, existe un menor desvalor jurídico en la conducta que nos lleva a subsumirla en la falsificación de documento privado del art. 395 CP.<sup>71</sup>

No obstante, lo anterior, volvemos a encontrarnos en este caso con un concurso de leyes entre el delito de falsificación de documento privado del artículo 396 y el delito de estafa hiperagravado analizado *ut supra*, y es que la aplicación de ambos supuestos unidos en virtud de un concurso medial vulneraría la prohibición del *non bis in idem*. Este tratamiento de la conjunción entre el art. 395 CP y la estafa ha quedado avalado por el Tribunal Supremo entre otras en la sentencia 975/2002 de 24 de mayo al señalar que «la condena por ambos delitos no es posible cuando la falsedad en el documento privado haya incidido en el tráfico jurídico exclusivamente como instrumento provocador del engaño que constituye el elemento nuclear de la estafa [...] la falsificación de un documento privado [...] sólo es delito cuando se realiza para perjudicar a otro. Si el perjuicio es de carácter patrimonial y da lugar a un delito contra el patrimonio como la estafa, la falsedad que formaría así parte del engaño, núcleo del delito de estafa, no podría ser sancionada junto a éste so pena de castigar dos veces la misma infracción [...] En cuanto a la pena aplicable, el artículo 8.4 del Código Penal dispone que el precepto penal más grave excluirá los que castiguen el hecho con pena menor».<sup>72</sup>

*Caeteris Paribus*, la aplicación de la regla de la alternatividad contenida en el artículo 8.4 CP nos lleva a apreciar tan solo la estafa hiperagravada quedando la de la falsedad de documento privado del artículo 395 absorbida por aquélla.

## E) Del delito de defraudación de fluido eléctrico

---

<sup>71</sup> En cuanto a la naturaleza del Documento Nacional de Identidad, el artículo 8 de la LO 4/2015 de protección de la seguridad ciudadana acredita que el DNI es un documento “*es un documento público y oficial (...) con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular*”

<sup>72</sup> STS 975/2002 de 24 de mayo, FJ 3º (ECLI:ES:TS:2002:3703)



- V. Concorre finalmente un delito de defraudación de fluido eléctrico del artículo 255.1. 1º CP del que responderían en concepto de coautores penalmente responsables los acusados **ANTONIO, VITALY** y **JAVIER**.

Esta figura delictiva se consuma efectuando los sujetos activos una defraudación de fluido (en este caso eléctrico) valiéndose para ello de «mecanismos instalados para realizar la defraudación». En el caso que nos ocupa las diligencias de instrucción practicadas revelan de forma indubitada como los acusados habían dispuesto un enganche ilegal tal y como fue descubierto en el marco del registro de la nave de Alfajarín efectuado el 15 de julio de 2022. De esta manera los acusados estaban permanentemente conectados a la red y al mismo tiempo que consumían energía eléctrica de forma legal extraían igualmente electricidad de modo clandestino e indetectable para el proveedor Endesa.

Tratándose de un delito menos grave penado exclusivamente con multa, es necesario analizar por un lado el criterio individualizador de la pena y por otro la actividad probatoria necesaria para enervar la presunción de inocencia. Con relación a la primera, numerosas resoluciones han señalado que el criterio a seguir no es sino la cuantía de la propia defraudación. Así, la Audiencia Provincial de Jaén, en la sentencia 141/2022 de 21 de junio señalaba que «con respecto a la cuantía de la defraudación, al no existir un contador para determinar el consumo real, debe de realizarse una cuantificación indiciaria en base al consumo probable estimado por las necesidades de la explotación».<sup>73</sup> En este caso, los informes aportados por Endesa en sede de instrucción y que obran en autos acreditan un consumo ilícito de energía eléctrica estimado en 45.000 euros. Con relación a la cuestión del elemento probatorio necesario, tal y como ha establecido el Tribunal Supremo en el caso de la defraudación de fluido eléctrico es suficiente para enervar la presunción de inocencia «La actividad probatoria resulta de las conversaciones telefónicas, de las intervenciones de sustancia tóxica y de los cultivos inspeccionados, así como de las periciales sobre los consumos y la instalación de derivaciones eléctricas para la defraudación de energía para el cultivo del hachís».<sup>74</sup> Este razonamiento, si bien aplicado al caso de la defraudación de electricidad para la producción *indoor* de estupefacientes, es de

---

<sup>73</sup> SAP Jaén 141/2022 de 21 de junio FJ 3º (ECLI:ES: APJ: 2022:750)

<sup>74</sup> STS 907/2021 de 24 de noviembre FJ 5º (ECLI:ES:TS: 2021:4270)

plena aplicabilidad al caso que nos ocupa puesto que los acusados se dedicaban a obtener electricidad fraudulentamente a través de una toma ilegal siendo la finalidad del todo irrelevante, lo mismo da que se trate de producción de drogas o de criptomonedas. Así, la intervención de las conversaciones telefónicas entre los acusados **ANTONIO** y **VITALY** pone de manifiesto la existencia de una red de procesadores ASIC enganchada clandestinamente a la red eléctrica en la nave industrial de Alfajarín. Igualmente, en el marco del registro del día 15 de julio de 2022 se intervinieron materiales (cable de conexión, herramientas, regletas de clemas y demás útiles) destinados a la defraudación, así como el propio enganche ilegal. Por último, los informes de consumo legal de electricidad aportados por Endesa hacen imposible a la luz de las cifras que reflejan el mantenimiento de la operatividad de los procesadores ASIC (que requieren de un suministro de energía continuo y muy alto) sin el recurso a la defraudación, algo que demuestran las estimaciones aportadas por los peritos de Endesa durante la instrucción. Por todo ello se deduce de forma indubitada la existencia de esta figura penal.

### **TERCERO. - Circunstancias modificativas de la responsabilidad penal**

3ª. No concurre ninguna circunstancia modificativa de la responsabilidad al no incardinarse los hechos en ninguna de las previstas en el Código Penal

### **CUARTO. - Conclusiones**

4ª. Corresponde imponer:

- I) Por el delito de constitución de organización criminal que tiene por finalidad la perpetración de delitos graves previsto y penado en el art. 570 bis del Código Penal a cada uno de los acusados la **PENA DE 5 AÑOS DE PRISIÓN, ACCESORIA DE INHABILITACIÓN ESPECIAL PARA EL EJERCICIO DEL DERECHO DE SUFRAGIO PASIVO DURANTE EL TIEMPO DE LA CONDENA**
- II) Por el delito continuado de estafa propia agravada del art. 74.2 y del artículo 250.2 CP en relación con el artículo 248 CP a cada uno de los acusados la **PENA DE 7 AÑOS DE PRISIÓN, MULTA DE**

**VEINTIDOS MESES A RAZÓN DE 40 EUROS POR DÍA Y LA ACCESORIA DE INHABILITACIÓN ESPECIAL PARA PROFESIÓN, INDUSTRIA, OFICIO O COMERCIO DURANTE EL TIEMPO DE LA CONDENA**

- III) Por el delito de blanqueo de capitales del art. 301.1 CP a los acusados **ANTONIO y VITALY** la **PENA DE 5 AÑOS DE PRISIÓN Y MULTA DE 2.500.000 MILLONES DE EUROS A CADA UNO Y RESPONSABILIDAD PENAL SUBSIDIARIA EN CASO DE IMPAGO**
- IV) Por el delito de defraudación de fluido eléctrico del art. 255.1.1º CP a cada uno de los acusados la **PENA DE 10 MESES DE MULTA CON UNA CUOTA DIARIA DE 6 EUROS Y RESPONSABILIDAD PENAL SUBSIDIARIA EN CASO DE IMPAGO**
- V) En condición de consecuencias accesorias y de conformidad con las prescripciones del artículo 127 y siguientes del Título VI, Libro II, del Código Penal el **DECOMISO DE TODO BIEN, MEDIO O INSTRUMENTO** con los que se hayan preparado o ejecutado los delitos anteriormente analizados dejando a salvo la responsabilidad que a tenor de las exigencias de los actores civiles será exigida en un procedimiento ajeno al presente

Y el pago de las costas procesales a todos los acusados por partes iguales

**OTROSÍ DIGO:** Que para el acto del juicio oral este Ministerio Público propone los siguientes medios de prueba:

1º.- Interrogatorio de los acusados

2º.- Testifical de los siguientes testigos, cuya citación se interesa practique el órgano de enjuiciamiento:

Funcionarios del Cuerpo Nacional de Policía con Número de Identificación Profesional 67.892, 89.826, 95.268, 108.982 y 120.672.

D. Gabriel González de la Mata, propietario de la nave industrial sita en Alfajarín

**3º.-** Para el supuesto de que las defensas impugnaran los informes obrantes en autos:

Pericial sobre los efectos intervenidos en el marco de los registros domiciliarios efectuados el 15 de julio de 2022

Documental de lo obrante a los folios de la pieza de intervenciones telefónicas 15 al 18, 34 al 45, 48 al 49, 97 al 101, y de los folios de la causa principal 32 al 35, 56 al 59, 62, 67, 69, 325 al 330, 350 al 352, 389 al 394, la cual deberá practicarse en las sesiones del Juicio Oral por medio de la íntegra lectura de los mismos, salvo que la defensa de los acusados, por entenderse informada de su contenido, renuncie a ella expresamente de lo cual se tomará oportuna nota en el acta, y todo ello sin perjuicio de la obligación impuesta al órgano judicial en el artículo 726 de la Ley de Enjuiciamiento Criminal.

**Madrid, 25 de diciembre de 2022**

**EL FISCAL**

### **III.- REFERENCIAS:**

#### **A) Legislación aplicable:**

- Ley Orgánica 10/1995 de 23 de noviembre del Código Penal
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal
- Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponible [online] en: <https://www.boe.es/buscar/act.php?id=BOE-A-2022-12644> (Fecha de consulta: 30 de diciembre de 2022)
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Disponible [online] en: <https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737> (Fecha de consulta: 29 de diciembre de 2022)
- LO 4/2015 de protección de la seguridad ciudadana. Disponible [online] en: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-3442> (Fecha de consulta: 27 de diciembre de 2022)
- Circular de la Fiscalía General del Estado nº 2/2011 sobre la reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales. Disponible [online] en: <https://www.boe.es/buscar/doc.php?id=FIS-C-2011-00002> (Fecha de consulta: 29 de diciembre de 2022)
- 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. Disponible [online] en: [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2019-2442](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442) (Fecha de consulta: 28 de diciembre de 2022)
- Memoria Elevada al Gobierno de S.M., Capítulo III, Apartado 8, Fiscalía Especializada contra la Criminalidad Informática. Disponible [online] en:

[https://www.fiscal.es/memorias/memoria2022/FISCALIA\\_SITE/index.html](https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/index.html)

(Fecha de consulta: 28 de diciembre de 2022)

- Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre Monedas Virtuales (2016/2007 (INI)) Disponible [online] en: [https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228\\_ES.html](https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_ES.html) (Fecha de consulta: 27 de diciembre de 2022)
- Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo. Disponible [online] en: <https://www.boe.es/doue/2019/123/L00018-00029.pdf> (Fecha de consulta: 29 de diciembre de 2022)

## **B) Bibliografía:**

- BALMACEDA-HOYOS, G., «El Delito de Estafa: una Necesaria Normativización de sus Elementos Típicos», en *Revista Estudios Socio-Jurídicos*, Vol. 13, núm. 2, julio-diciembre de 2011
- DOPICO GÓMEZ-ALLER, J. «Estafa y Dolo Civil: Criterios para su Delimitación», en *Dereito*, Vol. 21, nº1, 2012
- GARCÍA NORIEGA, A., «Blanqueo y Anti-Blanqueo de Capitales» en *Como se Lava el Dinero y Cómo se Combate el Lavado*, Difusión Jurídica, 2010
- PÉREZ LÓPEZ, X., «Las Criptomonedas: Consideraciones Generales y Empleo de las Criptomonedas Como Instrumento de Blanqueo de Capitales en la Unión Europea y en España», en *Revista de Derecho Penal y Criminología*, 3ª Época, nº. 18, julio de 2017
- PÉREZ MEDINA, D., «Blockchain, Criptomonedas y los Fenómenos Delictivos: entre el Crimen y el Desarrollo», en *Boletín Criminológico del Instituto Andaluz*
- MARÍN DE ESPINOSA CEBALLOS, E., «La Responsabilidad Criminal de los Miembros de una Organización o de un Grupo Criminal (arts. 570 bis y 570 ter CP): ¿un Problema de Autoría y Participación o de Tipicidad?» en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 24-25, 2022

- MOSER, M. et al. «An Empirical Analysis of Traceability in the Monero Blockchain», en *Privacy Enhancing Technologies Symposium*, abril de 2018, ps. 15 y 16
- SAINZ CANTERO, J.A., «El Delito Masa», en *Anuario de Derecho Penal y Ciencias Penales*, Fascículo 3, 1971
- SEGURA RAMÍREZ, S., «Anonimato en blockchain: Monero», Trabajo de Final de Grado, Universitat Politècnica de Catalunya, julio de 2020, p. 21 y sigs Disponible [online] en: <https://upcommons.upc.edu/bitstream/handle/2117/327128/memoria.pdf?sequence=1&isAllowed=y> (Fecha de consulta: 15 de noviembre de 2022)
- SERHACK & MONERO COMMUNITY «Mastering Monero, the Future of Private Transactions», ps. 61 y sigs, 129 y sigs. Disponible [online] en: <https://masteringmonero.com/> (Fecha de consulta: 23 de noviembre de 2022, si bien desde entonces el documento ha sido objeto de restricción de acceso requiriéndose del pago de una cantidad para su obtención)
- TSUCHIYA, Y., «Measuring Dark WebMarketplaces via Bitcoin Transactions: From Birth tú Independence», en *Forensic Science International: Digital Investigation*, mayo de 2020
- UNITED NATIONS OFFICE ON DRUGS AND CRIME, «Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies», june 2014, p. 27. Disponible [online] en: <file:///C:/Users/Usuario/Desktop/Crypto%20ML/Money%20Laundering/Manual%20UNODC%20Monedas%20virtuales.pdf> (Fecha de consulta: 28 de noviembre de 2022)

### C) Jurisprudencia

#### SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- STEDH de 22 de octubre de 2015, Skatteverket c. David Hedqvist, C-264/14, EU:C:2015:718. Disponible [online] en: <https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=ES> (Fecha de consulta: 27 de diciembre de 2022)

## **SENTENCIAS DEL TRIBUNAL SUPREMO**

- STS 907/2021, de 24 de noviembre (ECLI:ES:TS: 2021:4270)
- STS 326/2019, de 20 de junio (ECLI:ES:TS:2019:2109)
- STS 677/2019, de 23 de enero (ECLI:ES:TS:2020:148)
- STS 149/2017, de 9 de marzo (ECLI:ES:TS:2017:847)
- STS 371/2015, de 17 de junio (ECLI:ES:TS:2015:2758)
- STS 265/2015, de 29 de abril (ECLI:ES:TS: 2015:1925)
- STS 11/2015, de 29 de enero (ECLI:ES:TS:2015:393)
- STS 900/2014, de 26 de diciembre (ECLI: ES: TS: 2014: 5573)
- STS 166/2013, de 8 de marzo (ECLI:ES:TS: 2013:1110)
- STS 173/2013, de 28 de febrero (ECLI:ES:TS: 2013:921)
- STS 1035/2013, de 9 de enero (ECLI:ES:TS:2014:220)
- STS 974/2012, de 5 de diciembre (ECLI:ES:TS: 2012:8701)
- STS 839/2012, de 23 de octubre (ECLI:ES:TS:2012:7161)
- STS 778/2010, de 29 de julio (ECLI:ES:TS: 2010:5114)
- STS 356/2009, de 7 de abril (ECLI:ES:TS: 2009:2074)
- STS 416/2007, de 23 de mayo (ECLI:ES:TS: 2007:3596)
- STS 132/2007, de 16 de febrero (ECLI:ES:TS: 2007:1931)
- STS 50/2007, de 19 de enero (ECLI: ES:TS: 2007:1025)
- STS 507/2003, de 9 de abril (ECLI:ES:TS:2003:2509)
- STS 895/2003, de 18 de junio (ECLI:ES:TS:2003:4242)
- STS 975/2002, de 24 de mayo (ECLI:ES:TS:2002:3703)
- STS 353/2000, de 1 de enero (ECLI:ES:TS:2000:1615)
- Acuerdo No Jurisdiccional de la Sala 2ª del Tribunal Supremo, de 18 de julio de 2007 relativo a la unificación de criterios en torno a la penalidad del delito continuado de estafa y apropiación indebida

## **SENTENCIAS DE AUDIENCIAS PROVINCIALES**

- SAP Jaén 141/2022, de 21 de junio (ECLI:ES: APJ: 2022:750)
- SAP 166/2020, de 2 de junio (ECLI:ES: APM:2020:4742)
- SAP Madrid 704/2019, de 10 de octubre (ECLI:ES: APM:2019:4990A)
- SAP Santander 105/2021, de 30 de abril (ECLI:ES: APS: 2021:167)



- SAP de Madrid 505/2018, de 26 de junio (ECLI:ES:TS: 2019:3218) STS 276/2021, de 25 de marzo (ECLI:ES:TS:2021:1308)
- SAP de Las Palmas (Sección 1ª) 307/2017, de 13 de octubre (ECLI:ES:APGC:2017:1783)
- SAP Murcia 125/2014, de 22 de abril (ECLI:ES: APMU: 2014:955)

### **SENTENCIAS DE LA AUDIENCIA NACIONAL**

- Sentencia de la Sala de lo Penal de la Audiencia Nacional 35/2019, de 20 de diciembre (ECLI:ES:AN: 2019:4716)
- Auto 619/2022, de 3 de noviembre de la Sección 4ª de la Sala de lo Penal de la Audiencia Nacional (ECLI:ES:AN: 2022:9718A)
- Auto 241/2021, de 30 de junio de la Sección 3ª de la Sala de lo Penal de la Audiencia Nacional (ECLI:ES:AN:2021: 5372A)