LAS CRIPTOMONEDAS Y SU USO ILÍCITO EN EL BLANQUEO DE CAPITALES. CUESTIONES TEÓRICAS Y PRÁCTICAS.

José Joaquín Taús Ballester

Fiscal de la fiscalía provincial de Castellón

Blanqueo de capitales: persecución transfronteriza de activos. Retos que suponen las criptomonedas en el blanqueo de capitales

14 de marzo de 2024

SUMARIO

RESUMEN

La esencia del delito de blanqueo de capitales se encuentra en la ocultación del origen de ilícito de los bienes, dándoles apariencia de legalidad para, de esta forma, introducirlos nuevamente en el mercado como productos legítimos, pudiéndose definir por ello el delito de blanqueo de capitales como el hecho que pretende "la integración en el sistema económico legal de los beneficios obtenidos del delito"[1]. A lo que aspira este delito, es poner las máximas barreras al seguimiento de la huella del dinero fraudulentamente obtenido, y ello porque en caso de poder dibujar la trazabilidad del bien, dicho rastro nos conducirá, inexorablemente, tanto al producto del dinero como al delincuente.

Desde que a finales de la primera década del año 2000 surgieran las criptomonedas, su fama llamó la atención de los delincuentes, por cuanto estos activos presentaban unos caracteres que los convertían en especialmente apetecibles para los criminales.

El que el cobro del producto del delito en criptomonedas constituya con frecuencia un primer paso en este proceso de lavado de activos no es irrelevante, por cuanto el anonimato y la dificultad para el trazado de las criptomonedas constituyen un punto de partida idóneo para la ocultación de la estela del producto del hecho ilícito[2].

Por ello, el objetivo de este trabajo es tratar de aportar unas pinceladas sobre el delito de blanqueo de capitales a través de criptomonedas e intentar exponer la forma de abordar una investigación en la que tengamos constancia que las personas investigadas pueden ser titulares de criptomonedas.

Se pretende eliminar los miedos que nos pueden surgir ante una investigación por delito de blanqueo de capitales, porque sólo con el abordaje directo de este tipo de pleitos, será posible profundizar en los problemas que plantean para así, desde la práctica, tratar de no repetir errores en los que podamos haber incurrido y obtener el mejor resultado posible en nuestra investigación.

En conclusión, se plantean diversas cuestiones, tanto teóricas como prácticas, relacionadas con las criptomonedas y su conexión con el delito de blanqueo de capitales, ofreciendo, en algunos supuestos, recomendaciones que, lógicamente, no pueden ser consideradas como una solución única, pero sí como una opción válida y ajustada a derecho.

[1] BLANCO CORDERO, I. "El delito de blanqueo de capitales", Aranzadi, Cizur Menor, 2022, p. 31.

[2] PÉREZ LÓPEZ, X., "El blanqueo de capitales a través de las criptomonedas", SANZ DELGADO E. y FERNÁNDEZ BERMEJO D., *Tratado de Delincuencia Cibernética,* Aranzadi SAU, Navarra, 2021, p 542.

1.- INTRODUCCIÓN

El 1 de noviembre de 2008, una persona o grupo de personas, bajo el pseudónimo de Satoshi Nakamoto[3], dieron el pistoletazo de salida a la primera criptomoneda, el bitcoin, siendo minado el primer bloque de la moneda el 3 de enero de 2009, lo que supuso el nacimiento del primer activo.

La grave crisis mundial que azotaba el sistema bancario supuso el caldo de cultivo perfecto para que la fama de la nueva criptomoneda, que se presentaba[4] como una alternativa al sistema monetario tradicional que no dependiese de terceros de confianza sino de la tecnología existente y de la criptografía, corriese como la pólvora, ofreciendo entre sus puntos fuertes, la seguridad y fiabilidad en la realización de transacciones directas entre personas.

Ahora bien, prácticamente desde su inicio se estableció un binomio, entre las criptomonedas y la delincuencia organizada y transnacional, que todavía hoy perdura a modo de matrimonio perfecto, en el que los delincuentes, han encontrado, al fin, una manera de blanquear las ganancias obtenidas, con un grado de anonimización muy elevado, incluso, en ocasiones absoluto.

Y es que estos nuevos activos que habían surgido de la nada, las criptomonedas, presentaban unos caracteres tan sugerentes desde el punto de vista de las organizaciones criminales transnacionales, y también para los delincuentes de menor escala, que resultaba difícil no caer en la tentación de hacer un uso indebido de los mismos para lavar los activos obtenidos de manera ilícita.

No obstante, no fue hasta la segunda mitad de la década pasada, y como consecuencia de las investigaciones llevadas a cabo a raíz de los ataques terroristas que afectaron al territorio europeo (Barcelona y Niza, entre otros), cuando el legislador europeo tomó conciencia de la concreta relación existente entre las criptomonedas y la financiación del terrorismo y el blanqueo de capitales, lo que supuso la puesta en marcha de la maquinaria legislativa, con la finalidad de poner cerco al empleo ilícito de estos activos.

Desde el plano internacional, el GAFI[5] emitió diversos informes en los que, si bien se reconocía alguno de los beneficios de las monedas virtuales, también se puso el foco en los

---

[3] NAKAMOTO, S. "Bitcoin: Un Sistema de Efectivo Electrónico Usuario a usuario", https/bicoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

[4] CEDIEL A., y PÉREZ POMBO E.A., "Fiscalidad de Bitcoin, monedas virtuales y tokens", Editorial Atelier, 2023, pp 15-16.

[5] El GAFI, por sus siglas en inglés FATF (Financial Action Task Force) es un organismo internacional carente de personalidad jurídica internacional, pero que sí cuenta con una estructura orgánica. Se creó en 1989 por el G-7, con la intención de evaluar la cooperación ya iniciada para prevenir el uso del sistema bancario y financiero internacional como medio de blanqueo de capitales. En 1990 emitió un informe que contenía 40 Recomendaciones para ensamblar un sistema internacional de lucha contra el blanqueo de capitales.

riesgos que acompañan a los mismos, destacando entre esos dictámenes las Directrices para un enfoque basado en el riesgo de las monedas virtuales, del año 2015, el informe sobre activos virtuales y señales de alerta de 2018, con sus respectivas actualizaciones de los años 2019 y 2021.

En el ámbito europeo, se dictaron de manera sucesiva, la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión; la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, que aporta una definición de moneda virtual y también propone incluir en las legisladores nacionales a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos; la Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal, que conminaba a los estados miembros a introducir como circunstancia agravante del delito de blanqueo de capitales que la conducta ilícita fuera realizada por los sujetos obligados; y la Directiva de la UE 2019/713 del Parlamento de Europa y del Consejo, de fecha 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.

A pesar de todos estos esfuerzos legislativos, la Comisión Europea presentó el 14 de abril de 2021, la Estrategia de lucha contra la Delincuencia Organizada 2021-2025 de la Unión Europea, en la que indicaba que "*Pese a los avances de los marcos jurídicos destinados a luchar contra el blanqueo de capitales y recuperar activos, solo se detecta un pequeño porcentaje de las actividades de blanqueo de capitales, y únicamente se confisca el 1 % de los activos de origen delictivo. Esta situación se ha agravado con el uso cada vez mayor de canales financieros sometidos a una vigilancia más limitada que la del sector bancario, como las monedas virtuales.*" Advirtiendo además que existían, en los estados miembros, divergencias en su aplicación y deficiencias en el cumplimiento, por lo que se consideró necesario reforzar, tanto el cuerpo normativo que sobre la materia existe en la Unión, como los recursos personales de los que disponemos, ya que los cuerpos de seguridad no poseen las capacidades necesarias para llevar a cabo estas investigaciones complejas y onerosas.

Desde el punto de vista normativo, diversos son los textos legislativos que están pendientes de ver la luz, estando unos en una fase más embrionaria que otros. Así, podemos hablar de los siguientes trabajos:

1.- Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

2.- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se deroga la Directiva (UE) 2015/849

3.- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010.

4.- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos.

En la misma línea, puede mencionarse el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n. o 1093/2010 y (UE) n. o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, que, se espera, sea aplicable a partir del 30 de diciembre de 2024, si bien algunas disposiciones podrían estar ya vigentes el 30 de junio de 2024.

Este Reglamento pretende establecer una serie de normas uniformes, para los emisores de criptoactivos y para los proveedores de servicios en relación con dichos criptoactivos, que, *a grosso modo*, buscan dotar de transparencia y seguridad al mercado cripto.

El objetivo principal de la normativa será garantizar que las transferencias criptográficas, se puedan rastrear y bloquear aquellas que resulten sospechosas. La llamada *travel rule* cubrirá en el futuro las transferencias de activos criptográficos, de modo que la información, sobre la fuente del activo y su beneficiario tendrá que viajar con la transacción y almacenarse en ambos lados de la transferencia[6].

2.- CUESTIONES TEÓRICAS SOBRE LAS CRIPTOMONEDAS.

A continuación, con la finalidad de enfrentarnos con los mejores conocimientos posibles a las cuestiones prácticas que nos puedan surgir en el curso de un procedimiento, se tratará de explicar algunas cuestiones teóricas sobre las criptomonedas.

No se pretende analizar ni la estructura de bloques, ni la forma de creación de las criptomonedas, ni sus sistemas de seguridad; simplemente, se pretende una aproximación sobre qué son y también, sobre qué no son, para de esta forma, comprender cómo actuar sobre ellas.

2.1.- ¿QUÉ SON LAS MONEDAS VIRTUALES?

Desde el surgimiento del bitcoin, han sido múltiples las instituciones, tanto europeas como internacionales, que han intentado dar una definición acerca de qué debe entenderse por moneda virtual.

[6] JUEGA CUESTA, J., Criptoactivos y monedas virtuales: marco regulatorio y tributación, Editorial Lefebvre-El Derecho, S.A., Madrid, 2023, p.80.

En el marco internacional, el GAFI ha tratado de arrojar luz. En su informe del año 2015 sobre monedas virtuales "directrices para un enfoque basado en el riesgo", las describe como "*una representación digital de valor que puede ser comerciada de manera digital y funciona como un medio de intercambio; y/o una unidad de cuenta; y/o un depósito de valor, pero no tiene estatus de moneda de curso legal (es decir, cuando se presenta a un acreedor, es una oferta válida y legal de pago) en cualquier jurisdicción*". Añade que no es emitida ni garantizada por ninguna entidad y que cumple con las funciones anteriores sólo por acuerdo dentro de la comunidad de usuarios de la moneda virtual. Finaliza advirtiendo que la moneda virtual es distinta de la moneda fíat y del dinero electrónico.

En el plano europeo, varias son las entidades e instituciones que se han centrado en la materia. El Banco Central Europeo abordó su definición en el año 2012 determinando que se trataba de: "*Un tipo de dinero digital no regulado, que es emitido y, generalmente controlado por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual específica"*.

Dicha definición fue posteriormente matizada, y en el año 2015 aportó una nueva definición de la moneda virtual como *"Una representación digital de valor, no emitida por ninguna autoridad bancaria central, institución de crédito o emisor de dinero electrónico reconocido, que, en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero"*. Se pretendía así, diferenciarlo del dinero.

También el Parlamento Europeo se ha pronunciado al respecto mediante su labor legislativa. La Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, define las monedas virtuales como una "*representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*".

La Directiva de la UE 2019/713 la conceptúa como una "*representación digital de valor que no ha sido emitida ni está garantizada por un banco central ni por una autoridad pública, no está necesariamente asociada a una moneda de curso legal ni posee la condición jurídica de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*"

La primera de estas dos definiciones es asumida también dentro de nuestra legislación nacional por la Ley de Prevención de Blanqueo de Capitales que, en su artículo 1.5, describe la moneda virtual como "*aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente*". Es lo lógico, este concepto se introduce en la normativa administrativa por el Real Decreto Ley 7/2021, de 27 de abril, de transposición de directivas de la Unión

Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medias tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios trasnacionales y defensa de los consumidores.

Por último, también el Tribunal Supremo (en adelante TS) ha dado una definición sobre la materia, en concreto del bitcoin, en su STS 326/2019 de 20 de junio definiéndolo como "*un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica, 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*" añadiendo posteriormente que "*tampoco el denominado bitcoin es algo susceptible de retorno, puesto que no se trata de un objeto material, ni tiene la consideración legal de dinero*" insistiendo más tarde, al remarcar que "*permite utilizar al bitcoin como un activo inmaterial de contraprestación o de intercambio en cualquier transacción bilateral en la que los contratantes lo acepten, pero en modo alguno es dinero, o puede tener tal consideración legal, dado que la Ley 21/2011, de 26 de julio, de dinero electrónico, indica en su artículo 1.2 que por dinero electrónico se entiende solo el " valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico* ".

Para finalizar con el acercamiento a las monedas virtuales y a modo de curiosidad, hay que señalar que se está estudiando, por parte del Banco Central Europeo y los bancos centrales nacionales, la posibilidad de emitir un euro digital, que sería una moneda digital de banco central, un equivalente al electrónico al efectivo disponible para pagos en tiendas, en internet o entre particulares[7].

2.2.- ¿QUÉ SON LAS CRIPTOMONEDAS?

No debemos confundir el concepto de moneda virtual con el de criptomoneda. Las criptomonedas son una moneda virtual convertible descentralizada, basada en la matemática y que está protegida por criptografía, es decir, incorpora principios de la criptografía para implementar una economía distribuida, descentralizada y segura de información.

Las criptomonedas dependen de claves públicas y privadas para transferir el valor de una persona (individuo o entidad) a otra, que se encuentran matemáticamente relacionadas.

Las criptomonedas cuentan con diversas características diferenciadoras respecto a los sistemas tradicionales. No están reguladas ni controladas por ninguna institución y no requieren de intermediarios en las transacciones. No cuentan con un respaldo de un banco

[7] Toda la información referente a este proyecto del euro digital podemos consultarla en el siguiente link: https://www.ecb.europa.eu/paym/digital_euro/html/index.es.htm

central y ni de otras autoridades públicas y no están cubiertas por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversiones[8].

Con relación a bitcoin, la criptomoneda más conocida, El Salvador fue el primer país que la admitió como moneda de curso legal. este activo ha alcanzado tanta popularidad y ha copado tanto el mercado, que se usa el término Altcoin para referirse, de manera genérica, a todas aquellas cripto-monedas que no son bitcoin.

2.3.- ¿PUEDEN SER CONSIDERADAS DINERO?

En base a las definiciones expuestas, si hay algo claro, es que las monedas virtuales, entre las que se encuentran las criptomonedas, no pueden ser consideradas dinero.

Ya en el año 2014, la Directiva (UE) 2014/62 del Parlamento Europeo y del Consejo, de 15 de mayo, relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo, en su artículo 2, da una definición de moneda que choca frontalmente con uno de los principios básicos de las criptomonedas, que es su huida de cualquier tipo de intervencionismo y su carácter descentralizado.

También, la definición aportada por el TS, en relación con el bitcoin, deja claro que no es dinero, al recoger aseveraciones del tipo *"…ni tiene la consideración legal de dinero…*" y *"…en modo alguno es dinero…"*

Y no son dinero porque no reúnen muchas de las características de aquel. Así, no es obligatorio aceptarlas como medio de pago de deudas u otras obligaciones, su circulación es muy limitada y su valor oscila fuertemente, por lo que no pueden considerarse un buen depósito de valor ni una unidad de cuenta estable.

A lo anterior cabe añadir que tampoco cuentan con el respaldo de un banco central ni de otras autoridades públicas y que no están cubiertas por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversores.

Ahora bien, el hecho de no ser consideradas dinero no ha obstado para que haya comenzado desde hace tiempo, hablamos de bitcoin, a ser utilizada como medio de operaciones comerciales[9] y ello pese a que su valor no depende del precio del oro ni de otra moneda de curso legal[10].

---

[8] GUDÍN RODRÍGUEZ-MAGARIÑOS, F., Criptoactivos: de la paralegalidad a la paulatina legalización, Editorial Jurídica Sepin, Madrid, 2022, p. 27

[9] PÉREZ BERNABEU, B., "La administración tributaria frente al anonimato de las criptomonedas: la seudonimia del Bicoin", *Documentos-Instituto de Estudios Fiscales*, nº10, 2018, pag 150.

[10] GÓMEZ INIESTA, D.J., " Utilización de las nuevas tecnologías en la comisión del blanqueo de dinero", en ABEL SOUTO, M., y SÁNCHEZ STEWART, N. V Congreso sobre Prevención y Represión del Blanqueo de Dinero: Ponencias y conclusiones del congreso sobre las reformas de 2015 e incidencia en la economía y sociedad digital, Tirant lo blach Online, 2018, p. 1

2.4.- ¿CUÁL ES SU NATURALEZA JURÍDICA?

Con relación a esta cuestión existen, básicamente, dos posiciones. Por un lado, la que la considera como un elemento equiparable al dinero; dentro de las cuales los hay que las equiparan a una divisa virtual[11], pero también quienes, si bien las equiparan al dinero desde un prisma económico, destacan que, desde el jurídico, no puede haber equivalencia de conceptos, entendiendo que podría ser equiparable con dinero electrónico no regulado[12].

Por otro lado, están quienes explican las monedas virtuales por medio de los arts. 335, 337 y 345 de nuestro CC y las conciben como bienes muebles susceptibles de apropiación, fungibles y no susceptibles de copia[13].

Como vemos, la cuestión acerca de la naturaleza jurídica de las monedas virtuales no está resuelta y probablemente dependerá de cómo se vayan desarrollando los criptoactivos.

También desde el punto de vista procesal podremos considerarlos como efectos judiciales, de conformidad con lo dispuesto en el artículo 367 de la Lecrim.

2.5.- ¿POR QUÉ RESULTAN TAN APETECIBLES A LOS DELINCUENTES?

Prácticamente desde su origen, las criptomonedas se han vinculado con la delincuencia, formando un binomio que tiene su razón de ser en alguna de las características más evidentes de estos activos virtuales[14]:

- En primer lugar, el principio de descentralización que informa el sistema, que implica la ausencia de mecanismos de supervisión de las transacciones.

- En segundo lugar, las criptomonedas ofrecen un grado de privacidad de las transacciones elevado, dada la dificultad inherente al sistema para relacionar una transacción determinada con un usuario concreto y para trazar el camino seguido por una unidad de valor concreta que cambia de propietario. Existen algunas criptomonedas con un grado de privacidad importante, pero que no resulta imposible seguir el rastro con ciertos límites. En cambio, hay otras criptomonedas como, por ejemplo, monero, que sí que se promocionan como un tipo de criptomoneda con un anonimato técnicamente impenetrable.

---

[11] PEDREIRA MENÉNDEZ, J., *"La contabilización y tributación de la moneda digital (Bitcoins)"* IEF, Documentos de trabajo 20/2018 (1.ª parte), pág. 144

[12] NAVAS NAVARRO, S., "Un mercado financiero floreciente: el del dinero virtual no regulado (Especial atención a los Bitcoins)" *Revista CESCO de Derecho de Consumo*, n.º 13, 2015, pág. 90.

[13] CASANUEVA CAÑETE, D. y LÓPEZ DE LA CRUZ, N., "*El concepto de criptomoneda y breves consideraciones en torno a su tributación", p.* 79-80

[14] PÉREZ LÓPEZ X., "Las criptomonedas: consideraciones generales y empleo de las criptomonedas con findes de blanqueo", FERNÁNDEZ BERMEJO, D., Blanqueo de capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas, Editorial Aranzadi SAU, Navarra, 2019, p. 94-97

- En tercer lugar, también resulta estimulante para los delincuentes la irreversibilidad de las transacciones en algunas de las criptomonedas más importantes. Esta irreversibilidad no sólo favorece los pagos de víctima a delincuente, por cuanto hace posible un pago a distancia y no anulable a posteriori, sino que además dificulta la labor de su investigación que ven reducidas las posibilidades de intervenir una transacción.

- En cuarto lugar, en cuanto a fenómenos digitales que son, las criptomonedas se amoldan a las características clásicas de la ciberdelincuencia, la instantaneidad, la distancia entre el infractor y el lugar de comisión de una parte del iter del delito, carácter transfronterizo, con la problemática asociada a la jurisdicción competente y a la cooperación internacional. A este respecto, la navegación en la red causa la inevitable sensación de moverse sin frenos, sin restricción de ningún género y, sobre todo, sin que se atisbe en ninguno de los rincones que se visitan el menor rastro de los poderes públicos o privados convencionales[15].

- En quinto lugar, otra característica de las criptomonedas es su flexibilidad. Toda vez que pueden moverse fácil e instantáneamente por la red.

2.6.- ¿QUÉ SON LOS WALLETS Y LOS EXCHANGES?

El wallet, es el software que custodia las claves privadas que se precisan para acceder a las criptomonedas registradas en una dirección o clave pública para usarlas. Cabe tener presente que los wallets no custodian las criptomonedas, sino que contienen las claves para acceder al saldo de criptomonedas.

Pueden existir varias clases de monederos:

-Los monederos fríos "cold wallet", que reciben esta denominación porque no están continuamente conectados a internet. Pueden ser en papel o alojarse en un hardware.

-Los monederos calientes "hot wallet", así considerados porque precisan de una continua conexión a internet. Podemos distinguir también de tres tipos: las web wallets, que son online wallets basadas en sitios web resultando imprescindible acceder a una URL para acceder a la wallet; las mobile wallets, que son aplicaciones para teléfonos móviles donde se controlarán las claves privadas y las desktop wallets, diseñadas y construidas para ser instaladas y ejecutadas desde un ordenador.

Por lo que a los Exchange se refiere, se trata de plataformas en las que se puede comprar, vender o intercambiar las criptomonedas, a cambio de dinero fiat u otras criptomonedas. En ocasiones, estos proveedores de servicios también pueden ofrecer servicio de custodia de claves.

2.7.- ¿CUÁL ES LA POSICIÓN DE LOS WALLETS Y EXCHANGE EN EL DELITO DE BLANQUEO DE CAPITALES?

[15] MUÑOZ MACHADO, S. "La regulación de la red. Poder y derecho en internet, Editorial Taurus, Madrid, 2000, p. 35.

Como ya hemos indicado, la Unión Europa, al no vivir de espaldas a la problemática que las monedas virtuales están generando en el ámbito del delito de blanqueo de capitales ha dictado dos directivas, la Directiva (UE) 2018/843 y la Directiva (UE) 2018/1673, que atacan ya de manera directa, aunque probablemente no de forma suficiente, a su uso indebido, y cuya transposición al ordenamiento jurídico español, ha supuesto la introducción de la regulación, tanto en la normativa administrativa como penal, de los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, ("exchangers") y los proveedores de servicios de custodia de monederos electrónicos (en adelante "wallets), tratando de construir unos diques sólidos con los que atacar el anonimato de las criptomonedas y con ello, su uso en las actividades delictivas y, en especial, en el delito de blanqueo de capitales[16].

Fue la LO 6/2021 de 28 de abril, complementaria de la Ley 6/2021, de 28 de abril, por la que se reforma la Ley 20/2011, de 21 de julio, del Registro Civil, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y también de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal la que modificó los artículos 301.1 in fine y 302.1 in fine del Código penal, en el sentido de incluir dos párrafos nuevos, con los que, como ya hemos expuesto, se pretende completar la incorporación a nuestro ordenamiento jurídico del contenido de la Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal.

La modificación que afecta al segundo párrafo, es la que tiene interés para el presente trabajo, por cuanto introduce una nueva agravante vinculada a la especial condición del sujeto activo del delito de blanqueo de capitales, incluyendo como posibles sujetos activos del delito aquellos que, conforme a la normativa de prevención del blanqueo de capitales, tengan la condición de "sujetos obligados", entre los cuales se encuentran los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos, siendo éste el motivo por el que se dice la reforma referida coloca en el foco del delito de blanqueo de capitales a los "*wallets*" y a los "*exchangers*", sacándolos de esa zona sombría en la que, hasta la fecha, se estaban moviendo.

La inclusión de estos proveedores de servicios como sujetos obligados tiene una importancia, en teoría fundamental, pero en la práctica muy relativa.

A partir de este momento, los proveedores de estos servicios, en cuanto sujetos obligados conforme a la LPBC, están obligados a llevar a cabo ciertas obligaciones. Así, deberán aplicar un canon de diligencia en las operaciones, partiendo de los factores de riesgo que rodeen la operación, distinguiendo entre medidas de diligencias normales, medidas simplificadas o medidas reforzadas. Además, entre otros aspectos, deberán informar, con independencia de su cuantía, de cualquier operación u hecho, que pueda estar relacionado con el blanqueo de capitales, debiendo prestar especial atención a aquellas operaciones complejas, inusuales o sin un propósito económico o lícito aparente, o que presente indicios de simulación o fraude, comunicación que efectuarán al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

[16] TAÚS BALLESTER, J.J., "La responsabilidad penal de los wallets y los exchange dentro del delito de blanqueo de capitales", Diario La Ley, número 10346 de 12 de septiembre de 2023.

A modo de ejemplo, la normativa administrativa, entiende que deben aplicarse "*medidas reforzadas en relación con los países que presenten deficiencias estratégicas en sus sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo*" (art.11, apartado 1 de la Ley 10/2010, de 28 de abril) y "*figuren en la lista de terceros países que presentan deficiencias estratégicas en sus sistemas nacionales de lucha contra el blanqueo de capitales y la financiación del terrorismo, y que planteasen amenazas importantes para el sistema financiero de la Unión*".

De similar manera, el art.19 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, identifica en su apartado 2.e) que, entre los supuestos en los que los sujetos obligados aplicarán medidas reforzadas de diligencia debida se encuentran las "*Relaciones de negocio y operaciones con clientes de países, territorios o jurisdicciones de riesgo, o que supongan transferencia de fondos de o hacia tales países, territorios o jurisdicciones, incluyendo en todo caso, aquellos países para los que el Grupo de Acción Financiera (GAFI) exija la aplicación de medidas de diligencia reforzada".*

Para finalizar, el propio GAFI, en su informe sobre "*Activos virtuales, señales de alerta de lavado de activos y financiación del terrorismo*", establece una serie de alertas que deberán tenerse en cuenta cuando se dude del origen lícito de la transacciones de cripto-monedas, estableciendo seis grandes bloques, según estén relacionadas con las operaciones, con los patrones de la operación, con el anonimato, sobre remitentes o beneficiarios, en la procedencia del recurso o patrimonio y relacionadas con los riesgos geográficos.

Entre las señales de alerta que fija el GAFI, en relación con las operaciones, se encontraría el realizar múltiples operaciones de alto valor en una breve sucesión de tiempo, sin otras operaciones registradas durante un largo periodo y a una cuenta creada recientemente; trasferir activos virtuales a múltiples proveedores de servicios que no tengan relación con el lugar donde se vive. En cuanto a las señales de alerta referidas a los patrones de la operación se fijarían aquellas operaciones que involucren el uso de múltiples activos virtuales sin una explicación comercial lógica y el convertir una gran cantidad de moneda fiduciaria en activo virtual sin existir una explicación comercial clara. También existen señales de alerta relacionadas con el anonimato, y así lo serían, entre otras, cambiar un activo virtual que opera en una cadena de bloques pública a otro que le brinden un mayor anonimato u operar en proveedores de servicios no registrados. Entre las señales de alerta referidas a los remitentes o beneficiarios tendríamos, entre otras muchas, crear múltiples cuentas separadas bajo nombres diferentes o efectuar transacciones desde direcciones de IP que no sean de confianza. Por último, con relación a la procedencia de los recursos o patrimonio y alertas relacionadas con riesgos geográficos, podemos señalar como ejemplo de la primera el que las transacciones con cuentas de activos virtuales estén conectadas con esquemas de fraude y como ejemplo de la segunda que el cliente efectúe el cambio del activo virtual a dinero en una jurisdicción de alto riesgo con medidas inadecuadas de debida diligencia.

3.- SUJETOS INTERVINIENTES EN EL BLANQUE DE CAPITALES A TRAVÉS DE CRIPTOMONEDAS.

La nueva escenografía del delito de blanqueo de capitales, generada por la irrupción de las criptomonedas, ha supuesto un cambio en el panorama tradicional del lavado de activos,

provocando tanto el nacimiento de nuevos actores en la estructura criminal del ilícito como la adaptación de los tradicionales a las nuevas posibilidades de la delincuencia, hallándose el punto común de todos ellos en la proporción de un manto de anonimato en las operaciones con criptomonedas que es muy del gusto de los delincuentes, por cuanto obstaculiza seguir la estela de los activos blanqueados.

Ahora bien, debemos tener presente que al igual que afirmamos que la mera utilización de criptomonedas, en una transferencia económica, no puede ser suficiente para que, por si sola, tildemos la actuación como constitutiva de delito de blanqueo de capitales, lo mismo debe predicarse con el recurso a determinados proveedores de servicios que desarrollaremos con posterioridad (*trader, mixer, exchanger*….). Acudir a un mixer, por ejemplo, es indicativo de que el usuario de la criptomoneda busca anonimato, lo que, por sí solo, no puede ser considerado típico ni ilícito.

Será necesario analizar cada uno de los supuestos ante los que nos enfrentemos para poder determinar si la operación en cuestión es constitutiva o no de delito blanqueo de capitales mediante criptomonedas, pudiendo utilizar en estos supuestos, a modo de guía, el informe del GAFI sobre señales de alerta e indicativos de riesgo, al que ya hemos hecho referencia, pero también, los indicios clásicos utilizados para considerar que una determinada actuación puede ser constitutiva de delito de blanqueo de capitales[17], ya que el empleo de criptomonedas, en ocasiones, ha sido considerado, simplemente, como "*un medio para dificultar la investigación de las transacciones efectuadas*.[18]"

Cierto es que las criptomonedas son usadas habitualmente, sencillamente, por su aptitud para enmascarar las transacciones ilegales y obstaculizar su rastreo, pero también es cierto que precisamente estas circunstancias, son las que se convierten en un instrumento motivador para el blanqueo de capitales. Por ello, no será suficiente, para hablar de un delito de blanqueo de capitales cometido a través de criptomonedas, con acreditar que el sujeto ha hecho uso de ellas, ni tampoco que ha acudido a alguno de los actores que ahora analizaremos en sus transacciones económicas.

Es más, ni la concurrencia de una de las señales de alerta a las que se refiere el Gafi, podría ser suficiente, por sí sola, salvo las muy contundentes, para acreditar el delito de blanqueo de capitales, ya que será determinante analizar otros elementos que permitan un espectro más amplio sobre el riesgo de una determinada operación, debiéndose contextualizar la información obtenida de las autoridades pertinentes.

[17] En este sentido resulta ilustrativa la STS 225/2019 sobre los habituales indicios relacionados con el delito de blanqueo de capitales: *a) La importancia de la cantidad del dinero blanqueado,*

b) La vinculación de los autores con actividades ilícitas o grupos o personas relacionados con ellas, c) Lo inusual o desproporcionado del incremento patrimonial del sujeto, d) La naturaleza y características de las operaciones económicas llevadas a cabo, por ejemplo, con el uso de abundante dinero en metálico, e) La inexistencia de justificación lícita de los ingresos que permiten la realización de esas operaciones, f) La debilidad de las explicaciones acerca del origen lícito de esos capitales, g) La existencia de sociedades "pantalla" o entramados financieros que no se apoyen en actividades económicas acreditadamente lícitas"

[18] SAP de Lleida 308/2017, de 14 de junio.

Veamos, ahora, alguno de los protagonistas a los que hacíamos referencia:

3.1.- LOS MIXERS.

Es una herramienta cuya finalidad es, precisamente, mezclar las criptomonedas de unos usuarios con otros para lograr una mayor clandestinidad, para así, dinamitar cualquier huella pública de las mismas, lo que, lógicamente, hará difícil su trazabilidad.

Hay criptomonedas que no son totalmente anónimas ya que, a su paso, dejan una estela que puede incluir la data de la transferencia, el importe de los traspasos que se efectúen, las direcciones de los usuarios, etc. Es por ello, que en estas criptomonedas que no ofrecen un grado absoluto de privacidad, como el bitcoin, los usuarios pueden acudir a estos prestadores de servicios.

Con estos *mixers*, los usuarios, no obtienen la misma cripto-moneda que adquirieron. Todas las criptomonedas depositadas en los proveedores de estos servicios se mezclan entre sí en un cúmulo de pequeñas transacciones, obstaculizando la determinación de las criptomonedas afectadas.

Si bien es cierto que la mayoría de los usuarios que acuden a estos servicios de los mixers lo hacen para proteger su anonimato y no para fines ilícitos, lo cierto es que, por sus propias características, resulta sugerente a los criminales.

3.2.- LAS CRIPTOMULAS.

Las “criptomulas” tienen la misma forma de actuar que las mulas en el ámbito de la delincuencia tradicional.

En estos casos, las criptomulas serían empleadas para la apertura de cuentas en los *exchangers* para recibir los activos y posteriormente transferirlos a otra dirección que, generalmente, puede pertenecer ya a los delincuentes o a otras criptomulas, repitiendo la dinámica tantas veces cuantas barreras quieran interponer los delincuentes.

Estas criptomulas podrían prestar su colaboración de manera voluntaria, siendo además conscientes de que están interviniendo en una operación ilícita, pasando a formar parte del entramado delincuencial con pleno conocimiento de su participación y función, pero también de manera voluntaria, aunque desconociendo que están siendo instrumentalizados con un fin ilícito. En este último supuesto, habrá que estar al caso concreto para valorar su responsabilidad penal.

Por último, también podría darse la posibilidad de que la criptomula haya sido usada desconociendo ella absolutamente su participación, en caso de que la identidad de esta haya sido previamente suplantada. Al igual que la práctica diaria de los tribunales nos muestra incontables supuestos de aperturas de cuentas bancarias haciendo uso de documentación

personal obtenida previamente de otro sujeto, generalmente de manera indebida, de igual manera se podría operar con relación a las criptomonedas. Se podría abrir una billetera haciendo uso de esa documentación del tercero, con la que también posteriormente acudir a un Exchange, para convertir la criptomoneda en dinero fiat que transferiríamos a esta cuenta bancaria abierta también de manera ilícita.

3.3.- LOS LOCAL TRADER.

Como su propio nombre indica, estamos, en este caso, en presencia de un comerciante que se dedica a la compra de monedas virtuales y que, cuando las condiciones de mercado lo aconsejan, procede a su posterior venta para, en base a la volatibilidad que preside este marco financiero, obtener ganancias.

En este supuesto, los delincuentes podrían acudir al servicio para lograr una especie de plusvalía de sus ilícitas ganancias, ya que no procederían a la inmediata transformación en dinero fiduciario, sino que acudirían a un servicio que custodiaría la criptomoneda con la expectativa de que aumentará su valor y, entonces, proceder a su venta. Sería un caso de ganancia sobre ganancia que, además, separaría la ulterior venta de la criptomoneda del hecho ilícito, lo que sería un obstáculo más para vincular a ambos.

Generalmente, estos sujetos, ofertan sus servicios en internet y el sistema de cambio suele sustentarse en el intercambio *(peer to peer).*

3.4.- LOS EXCHANGERS.

Se trata de proveedores de servicios de intercambio de moneda virtual por moneda fiduciaria, aunque también pueden ofrecer servicios de cambio de una moneda virtual por otra, habiendo hecho referencia a los mismo en el anterior bloque de esta ponencia.

Podemos encontrar exchange centralizados, que serán aquellos que, entre otros lugares, presten sus servicios en jurisdicciones con una legislación estricta y ajustada en materia de lavado de activos.

Por otro lado, también hallaremos exchange descentralizados (DEX) que desarrollan su actividad en paraísos fiscales o en otras jurisdicciones con una normativa más laxa en materia en blanqueo de capitales.

3.5.- LOS WALLETS.

Como ya hemos referido, los wallets son proveedores de servicios de custodia de monederos electrónicos. Su relevancia con relación al delito de blanqueo de capitales vendría determinada porque son los proveedores de servicio que custodian las claves de la criptomoneda.

En este sentido y analizándolas desde el prisma del delito de blanqueo de capitales, podría darse la situación de que quien apareciera como usuario del monedero fuera una tercera persona interpuesta, bien un hombre de paja del que se valga la organización criminal o bien

una persona a la que se le haya usurpado la identidad, con el único fin de no revelar quiénes son los auténticos propietarios de la criptomoneda.

3.6.- CRIPTOMONEDAS PRIVADAS.

Si bien muchas de las criptomonedas utilizadas en el ámbito virtual tienen carácter de pseudoanónimas, como ya hemos analizado, existen otras que, por las características de su protocolo, resultan de imposible trazabilidad, de manera que las transacciones que se efectúan en su blockchain, resultan del todo opacas, por lo que son utilizadas por aquellos usuarios que buscan oscuridad e intimidad, en sus operaciones. Dentro de ellas, monero, es la más conocida.

3.7.- TARJETAS DE CRIPTOMONEDAS.

Es una de las herramientas de la que disponen los usuarios de criptomonedas para acceder a ellas. Generalmente, suelen ser facilitadas como una prestación más de los exchange y su incidencia se limitaría a lo dicho con relación a los wallets, es decir, que la tarjeta figure a nombre de un tercero que ejercería de "hombre de paja".

3.8.- CAJEROS AUTOMÁTICOS DE CRIPTOMONEDAS.

Estos cajeros, generalmente, permitirán tanto la compra de criptomonedas como su venta.
Si lo que se quiere es obtener una criptomoneda, en primer lugar, habrá que seleccionar la que se quiere, de entre las que oferte el cajero; a continuación, se ingresará el dinero en efectivo en el cajero y se facilitará una dirección de monedero, de modo que confirmada ésta, las criptomonedas se transferirán a dicha billetera. En caso de no disponer previamente de una cartera, es posible que el cajero automático de criptomonedas la genere.

Si lo pretendido es la venta de la criptomoneda, el proceso será a la inversa. El inicio será la recepción de un mensaje de texto de verificación al móvil del usuario. Cuanto éste lo recibe, debe ingresarlo en la máquina para luego escanear la dirección del monedero del cajero y transferir las criptomonedas. Una vez que se confirme, el dispositivo desembolsará el efectivo.

4.- TIPOLOGÍAS DELICITIVAS DEL BLANQUEO DE CAPITALES A TRAVÉS DE CRIPTOMONEDAS.

A continuación, vamos a pasar a exponer algunos supuestos tradicionales de blanqueo de capitales, si bien introduciremos la peculiaridad de que el lavado de activos se llevará a cabo a través de criptomonedas. Y dado que, hasta la fecha, las sentencias sobre el particular son más bien escasas, ya avanzamos que nos moveremos en el campo de la hipótesis y de lo prospectivo.

4.1- COMPRA DE INMUEBLES.

Los bienes inmuebles han sido, tradicionalmente, el método estrella de aquellos delincuentes dedicados al blanqueo de capitales.

Podemos distinguir varios supuestos, según la cantidad entregada esté compuesta íntegramente por criptomonedas obtenidas de manera ilícita, algo que no tiene por qué saber el comprador, o bien que se entregue una parte del importe de la venta en moneda fiduciaria y otra parte en criptomoneda. Una vez los delincuentes procedan a la venta del inmueble adquirido con dichos criptoactivos, se habrá completado íntegramente el círculo del blanqueo de capitales.

Cabe tener presente que, aunque no se trate de una operación que incluya alguna señal de riesgo, el notario, conforme el artículo 2.1.n de la LPBC, es un sujeto obligado, por lo que si tiene dudas acerca del carácter fraudulento de la operación debería ponerlo en conocimiento de la autoridad supervisora.

4.2.- CREACIÓN Y DESARROLLO DE EMPRESAS PANTALLA

El delito de tráfico de drogas, el delito base más investigado con relación al lavado de activos, constituye una actividad punible con una clara finalidad económica, originadora de importantes cantidades de dinero susceptibles de ser lavadas a través de empresas pantalla.

El *modus operandi* en estos casos siempre es muy similar: constitución de una sociedad limitada con un capital social mínimo rondando los 3.000 euros, que en nuestro país es el mínimo de la Sociedad de Responsabilidad Limitada, sin haber depositado las cuentas anuales ante el Registro Mercantil y, por tanto, aparentemente sin que podamos atribuirle actividad comercial alguna, limitándose en muchos casos a ostentar la propiedad de bienes, especialmente inmuebles con los que operar. Las criptomonedas podrán ser aportadas al capital social.

Dado que el objeto social suele generalmente focalizarse en la tenencia, compra y venta de inmuebles, podría tratarse de una vuelta de tuerca del supuesto anterior. En el sentido de que los bienes inmuebles adquiridos, en todo o en parte, con criptomonedas, podrían ser posteriormente, en lugar de vendidos, aportados al capital social de una de estas empresas pantalla que, como es lógico, no tendrá a los auténticos delincuentes en la administración de la sociedad.

También es habitual el uso de establecimientos de restauración (bar, restaurantes, cafeterías…), con actividad comercial lícita que, con el fin de blanquear activos, se dedican a inflar la facturación del local. Este diferencial, entre lo realmente facturado y lo insuflado artificialmente, puede ser utilizado, al tratarse de un ingreso ilícito que se incluye indebidamente en las cuentas, para la adquisición de criptomonedas, cuya obtención el delincuente justificará, posteriormente, con la actividad comercial del establecimiento, lo que obligará a un minucioso estudio de sus cuentas para acreditar que, el dinero con el que se adquirieron los activos no procedía de la actividad lícita del local.

4.3.- COMPRA DE BIENES DE LUJO Y OBJETOS DE ARTE.

Este supuesto es también uno de los más habituales para la comisión del delito de blanqueo de capitales. Al igual que el blanqueador tradicional puede comprar objetos valiosos con el dinero obtenido de manera ilícita, también el ciber blanqueador que opere con criptomonedas puede ejecutar el delito.

El hecho podría ser realizado bien pagando el objeto directamente con criptomonedas obtenidas con la transformación del dinero obtenido de manera ilícita, o bien con dinero originado de la transformación de criptomonedas obtenidas ilícitamente o tras haber convertido el dinero originariamente delictivo en tales activos virtuales.

4.4.- COMPRA DE BILLETES DE LOTERÍA.

Al igual que la realización de esta compra es un modelo habitual en el blanqueo de capitales tradicional, donde el blanqueador entrega una cantidad sensiblemente superior a la del valor del premio obtenido por el particular, para así incentivar su venta, lo mismo podría predicarse respecto del blanqueo de capitales a través de criptomonedas.

En este caso, bastaría con que el blanqueador diera con el sujeto que hubiera obtenido el premio y ofrecerle, a cambio del boleto laureado, la criptomoneda de su titularidad, de manera que, en cuanto el delincuente cobrase el dinero derivado del billete premiado, habría conseguido blanquear aquello que, en origen, era ilícito.

4.5.- PLATAFORMAS DE JUEGO (PÓKER, CASINOS…) Y APUESTAS.

Las plataformas de juego son populares entre los blanqueadores de dinero en criptomonedas.

En estos supuestos, lógicamente, la obtención de una ganancia extra es algo residual para el delincuente. El blanqueador, apostará cantidades importantes de dinero, tras haber transformado sus criptomonedas en dinero fiat y dado el carácter aleatorio de las apuestas o de los juegos, será prácticamente imposible demostrar el origen delictivo del dinero.

Generalmente, suelen utilizarse muleros, ofreciéndoles unas cantidades de dinero residuales para los delincuentes, pero tremendamente atractivas para ellos. Los blanqueadores, que serán los apostadores reales, suelen estar en otros países, mientras que los muleros, también llamados en estos supuestos “zombis”, serán quienes efectuarán las apuestas con el dinero que reciban de los delincuentes.

Lógicamente, las cuentas que se abran en las plataformas no estarán a nombre de los blanqueadores sino que estarán a nombre de los muleros.

También es posible que, en lugar de muleros, los delincuentes usen los datos de personas cuya identidad, haya sido previamente usurpada.

Una vez la ganancia de la apuesta o del juego se ingresa en la cuenta abierta, el dinero ya estaría lavado y tendría status de legal.

El GAFI, en su informe de septiembre de 2020 "*los activos virtuales, bandera roja del blanqueo de capitales y la financiación del terrorismo*", señala varios usos de los activos virtuales, dentro de los que se encontrarían las criptomonedas, para blanquear, considerando como supuestos de "*bandera roja*", una basada en el anonimato, cuanto se refiere a fondos procedentes de billeteras relacionadas con fuentes sospechosas conocidas de mercados de *darknet*, servicios de mezcla o giro, apuestas, actividades ilegales o de estafas o robos, y una segunda relacionada con la fuente de los fondos o recurso al hablar de transacciones de activos virtuales con origen o destino en servicios sospechosos de juegos de azar en línea.

4.6.- PITUFEO.

Es posible que los beneficios económicos obtenidos como consecuencia de la actividad ilícita de los delincuentes sean invertidos en la compra de criptomonedas. Una vez adquiridas, podrían ser nuevamente transformadas en dinero fiat, haciendo uso para ello de cajeros de criptomonedas.

Una vez obtenido el dinero, los delincuentes podrían aperturar múltiples cuentas bancarias y hacer pequeños ingresos en efectivo en las mismas, también de manera periódica, para tratar de no activar las alarmas de las entidades financieras, introduciendo en el circuito legal dinero que, en su origen, era ilícito.

4.7.- COMPRA DE MATERIAL PARA LA MINERÍA DE CRIPTOMONEDAS.

Es posible que los delincuentes inviertan el producto económico ilícitamente obtenido en la compra del aparataje necesario para llevar a cabo labores de minería, para con ello, conseguir bitcoins que, posteriormente, podrían reinvertir en otros bienes.

Los equipos para llevar a cabo el minado, por ejemplo, de bitcoin, puede girar alrededor de los 4000 euros[19]. Si contamos con que los delincuentes gozan de la capacidad económica suficiente para construir auténticas granjas de minado, con múltiples de estos aparatos, en los que, además, habría que invertir una cantidad importante de dinero en insonorización, ya que toda la maquinaria necesaria es tremendamente ruidosa y que además, consumen una gran cantidad de energía, las ingentes cantidades de dinero obtenidas de una actividad delictiva previa, podría ser reinvertida de este modo para así, obtener nuevas criptomonedas, aparentemente legales.

[19] Precio en el que en la plataforma de Amazon se vende el Antminer S19 XP 141T SHA-256 Máquina Minera Bitcoin BTC

4.8.- LOS EXCHANGERS.

Podríamos distinguir aquí dos tipos de exchangers distintos. Los que se encuentran centralizados y los no centralizados, también conocidos como (DEX).

En el primer caso, se encontrarían aquellos Exchange que están sometidos a control por parte de las autoridades supervisoras en materia de blanqueo de capitales pero que, no respetan las exigencias legales del país en el que operan. En estos casos, los exchangers, no sólo serían responsables del incumplimiento de las exigencias administrativas correspondientes, con la amenaza de la correspondiente sanción, sino que podrían ser también, y así lo prevé el artículo 302.1. *infine* del código penal, autores del delito de blanqueo de capitales.

Y el incumplimiento de las obligaciones podría tener dos razones. Bien que el proveedor de servicios esté dominado totalmente por los delincuentes, en cuyo caso lo normal sería que el administrador sea un "hombre de paja" o bien que, siendo un proveedor legal con actividad regular, los delincuentes hayan conseguido seducirle para que no informen o no respeten las exigencias legales en las transferencias que les afecten.

En el segundo bloque, se encontrarían estos proveedores de servicios con sede en paraísos fiscales o en territorios con una regulación relajada. Estos exchange exigen poca o ninguna verificación de la identidad del usuario para transferir criptoactivos y, por tanto, son muy atractivos para los delincuentes, quienes podrán mover y transferir, sin problemas, sus cripto-monedas.

Ya hemos indicado que la Directiva (UE) 2018/843, imponía ciertas condiciones para los exchangers que operase en alguno de los países miembros de la Unión, pero no, para los países externos a la unión europea, por lo que la ubicación fuera de Europa es un atractivo para las organizaciones criminales que actúan con ellas, o que incluso, llegan a tomar su control, ante el escaso compromiso de colaboración, en el intercambio de información, con las entidades de control.

4.9.- PARAISOS FISCALES.

En España, el Ministerio de Hacienda y Función Pública publicó la Orden HFP/115/2023, de 9 de febrero, por la que se determinan los países y territorios, así como los regímenes fiscales perjudiciales, que tienen la consideración de jurisdicciones no cooperativas[20]. Esta Orden, además, adecua el término "paraísos fiscales" al concepto de "jurisdicciones no cooperativas" y amplía el concepto de paraíso fiscal, atendiendo a diversos criterios.

Por tanto, estaremos haciendo referencia, en estos supuestos, a aquellos casos en los que el sujeto activo del delito actúa con proveedores de servicios que encuentran su sede no sólo en paraísos fiscales sino también en aquellas jurisdicciones consideradas como no cooperativas,

[20] La Orden y la lista de jurisdicciones puede consultarse también en el link: Orden HFP/115/2023, de 9 de febrero, por la que se determinan los países y territorios, así como los regímenes fiscales perjudiciales, que tienen la consideración de jurisdicciones no cooperativas. (boe.es)

entendiendo por éstas a aquellas que presentan deficiencias en su legislación de lucha contra el blanqueo de capitales.

El Grupo de Acción Financiera Internacional (GAFI) identifica las jurisdicciones con medidas débiles de lucha contra el blanqueo de capitales y la financiación del terrorismo (ALD/CFT) en dos documentos públicos, que suelen denominarse externamente "lista negra" y "lista gris"[21]. La Comisión Europea también identifica a los países que presentan deficiencias estratégicas en sus regímenes de PBC/FT y que suponen una amenaza significativa para el sistema financiero de la Unión Europea[22].

Nada impide a los miembros de las organizaciones criminales, dadas sus potentes estructuras y la incalculable cantidad de dinero que mueven, residir en un determinado país y moverse a otro, incluso otro continente, para llevar a cabo el lavado de los bienes obtenidos indebidamente si con ello se asegura, una mayor flexibilidad en las operaciones.

5.- CUESTIONES PRÁCTICAS

Y una vez resueltas algunas cuestiones teóricas sobre las criptomonedas y tras haber expuesto también algunos de los sujetos que pueden intervenir en la nueva modalidad del blanqueo de capitales que estamos analizando, habiendo divagado incluso sobre algunas de las nuevas tipologías delictivas, procede ahora aportar una serie de ideas acerca de cuestiones que nos puedan surgir en un procedimiento penal seguido por delito de blanqueo de capitales mediante criptomonedas.

5.1.- ¿PODEMOS ADOPTAR MEDIDAS CAUTELARES REALES SOBRE LAS CRIPTOMONEDAS?

Rotundamente sí. Ya advertía la Circular de la FGE 4/2010 que "*evidenciándose que la intención última de los grupos delictivos organizados es la colocación en el "circuito legal" del producto de su actividad, para su utilización y disfrute en las mismas condiciones que si su procedencia fuera lícita, las nuevas estrategias de política criminal tienden a incidir en las ganancias producidas por el delito, procurando limitar el enriquecimiento y la capacidad económica de dichos grupos criminales*" y para ello, en la conclusión decimotercera se nos insta a que "*cuando a tenor de las actuaciones practicadas en las Diligencias de Investigación resulte indicado la adopción de medidas cautelares de afianzamiento y embargo para el aseguramiento de responsabilidades civiles (Instrucción FGE n.º 1/1992) o para la incautación de los objetos, efectos, instrumentos y ganancias, los Sres. Fiscales procederán a la inmediata judicialización de las mismas a los referidos efectos*"

[21] Puede consultar el listado en el siguiente link: https://www.fatf-gafi.org/en/countries/black-and-grey-lists

[22] La última versión del listado puede consultarse en el siguiente enlace: High risk third countries and the international context content of anti-money laundering and countering the financing of terrorism - European Commission (europa.eu)

De este modo, si la criptomoneda intervenida en las actuaciones puede ser considerada efecto del delito, el bien, medio o instrumento con el que se haya preparado o ejecutado o una ganancia procedente de tal ilícito, se deberá decomisar el activo, de conformidad con los artículos 127 y 301.5 del código penal. No hace falta esperar a la celebración del juicio para solicitar el decomiso toda vez que nuestro ordenamiento jurídico permite acordarlo como medida cautelar, conforme el artículo 127 octies del código penal.

En cambio, si no está relacionada con el delito que estamos investigando ni tampoco queda acreditado otro origen ilícito, pero, a través de su realización, pueden asegurarse responsabilidades civiles derivadas del hecho investigado, recordemos que estamos hablando de un delito de blanqueo de capitales en el que puede tener cabida un pronunciamiento sobre responsabilidad civil, por lo que procederemos a su embargo.

5.2.- ¿DÓNDE LOCALIZAR LAS CRIPTOMONEDAS?

Partamos de una premisa clara. La localización y la captura de las criptomonedas va a ser cuasi imposible si no contamos con la colaboración voluntaria y/o involuntaria de los usuarios.

Las criptomonedas pueden estar alojadas bien en un monedero frio o bien, en un monedero caliente. Y es posible, además, que para acceder a las claves tengamos que disponer, en primer lugar, de la frase semilla y esto, porque como estamos reiterando, una de las características de las criptomonedas es su seguridad y una de las llaves para lograrlo es a través del uso de frases semilla.

Una frase semilla no es más que un grupo de palabras usadas como claves secretas para acceder a una billetera de criptomonedas, constituyéndose en una forma de verificar la identidad del usuario y proteger a la billetera. La frase semilla, generalmente, será una secuencia de 12, 18 o 24 palabras, que se generan de manera aleatoria y se manifiestan al sujeto durante la fase de constitución de la billetera.

No podemos confundir la frase semilla con la clave privada. De una manera muy sencilla podríamos decir que la frase semilla protege la billetera y la clave privada la criptomoneda. En base a ello, la frase semilla permite el acceso a la billetera y, por tanto, a la totalidad de cuentas que el usuario tenga en el monedero. Por el contrario, cada clave privada está vinculada a una clave pública. De manera metafórica, con la frase semilla accedemos a la totalidad de nuestras cuentas bancarias, con la clave privada accederíamos a cada una de nuestras cuentas bancarias de manera individual.

En síntesis, si no tenemos la frase semilla, resultará complicado arrebatar las criptomonedas a los delincuentes, pese a que tengamos la certeza de que las poseen.

En el caso de que dispongamos de ella, bien porque la persona investigada nos la haya facilitado, bien porque la hayamos podido localizar de entre todo el material incautado, tendríamos ya la primera llave del laberinto que nos puede llevar a la captura de las criptomonedas de los delincuentes, por lo que pasaríamos a la siguiente fase, que será, la localización del lugar donde se hallan las claves, exponiendo varios supuestos que podrían ser los más habituales.

Apuntar, en este sentido, que, si en el curso de la investigados intuimos que los investigados pueden ser usuarios de criptomonedas, sería conveniente que, con carácter previo a explotar la operación, bien el Laj del juzgado, bien la policía judicial, procedieran a la apertura de una billetera, donde poder transferir la criptomoneda, en caso de ser localizada.

Las páginas más conocidas para su generación serán www.generatepaperwallet.com (para bitcoin, bitcoin cash, etherum…), www.xrppaperwallet.com (para XRP Ripple) y/o https://moneroaddress.org/ para generar la *paper wallet* para monero. Si bien estas URL no son las únicas, si llegamos con ellas al 87,11 % de la capitalización total del negocio de criptodivisas.

Además, también sería prudente que, en caso de solicitar la entrada y registro en los inmuebles dominados por los criminales, tal diligencia fuera acompañada, además de la habitual referencia a la aprehensión de equipos y materiales relacionados con el hecho investigado, de la petición de autorización judicial para acceder a los dispositivos que se localicen en el lugar de los hechos y/o, en poder de los delincuentes.

Pasamos ahora al análisis de alguno de los casos ante los que nos podemos encontrar:

1.- El primer supuesto sería, encontrarnos con una billetera de papel (paper wallet) en que fuera perfectamente visible la clave privada. En este supuesto parece claro que las posibilidades de éxito en la aprehensión serían elevadas. Ahora bien, la localización de dicho monedero no nos debe confundir. Con la localización de la billetera de papel, lo único de lo que disponemos, es de un papel en el que, por regla general, nos aparecerá la clave privada y pública de la criptomoneda. No tendremos todavía la criptomoneda.

Como cualquier papel, puede que haya sido objeto de fotocopias y que existan, por ello, más personas que dispongan del mismo documento. En este caso, resultará de vital importancia la rapidez en la actuación, por lo que una vez con el *paper wallet* en nuestro poder y con las claves de la criptomoneda, deberemos acceder a la aplicación correspondiente para una vez dentro, poder barrer dicha criptomoneda a la dirección pública que, como ya hemos indicado, tendríamos que haber abierto previamente. Una vez efectuada la transferencia a nuestra dirección pública, ya tendremos el activo en nuestro poder, describiendo, en la pregunta siguiente, las distintas formas de custodia que tendremos.

2.- Si el supuesto anterior consistía en la localización del *paper wallet* en buen estado, donde se observan perfectamente las claves, también puede ocurrir, como es lógico, que localicemos la billetera pero que la observación de las claves no sea posible, al aparecer uno/varios números borrados. En este caso, deberíamos ir probando, de manera aleatoria en esos números borrosos, por si la diosa Fortuna estuviese de nuestro lado y nos premiase con el descubrimiento de los números borrados. No es fácil que salga bien, ya que hay que tener en cuenta que, en la mayoría de las criptomonedas, hay un número máximo de intentos, que tampoco es excesivo, para corregir la clave introducida de manera errónea.

3.- Junto con el supuesto anterior, la tercera posibilidad sería la de encontrarnos la billetera en un hardware, que generalmente será un dispositivo USB. En estos casos, la posibilidad de

triunfo también es elevada. Habría que comportarse conforme a la manera descrita en el supuesto 1.

4.- Un cuarto supuesto podría ser que el investigado, tuviese la aplicación de la criptomoneda de la que es usuario abierta y nos facilitara las claves. Qué duda cabe que, en este supuesto, apresar la criptomoneda sería sencillo, debiendo también en este caso arrastrarla al llavero que deberíamos haber abierto previamente.

5.- Un quinto supuesto podría ser que el investigado, tuviese la aplicación de la criptomoneda de la que es usuario cerrada y no accediera a facilitarnos las claves. En ese caso, no sería posible la aprehensión de la criptomoneda.

6.- Localizar anotadas en algún documento las claves de la criptomoneda. En este caso deberemos actuar como en el supuesto 1. Será necesario una vez estemos en poder de las claves, acceder a la plataforma correspondiente para, una vez dentro, poder barrer la criptomoneda a la wallet que deberíamos haber abierto con carácter previo. Ahora bien, en caso de que para acceder a la plataforma fuera necesario una doble autentificación, podríamos también encontrarnos con el problema de que el investigado no coopere, con lo que las posibilidades de éxito se reducirán de manera considerable.

7.- También sería posible que el investigado tuviera custodiados sus criptoactivos en algunos de los wallets y/o exchangers registrados en España. Ante esta hipótesis, deberíamos librar oficio a la entidad de supervisión de estos proveedores para que nos faciliten la información acerca de si el/los investigado/s son titulares de alguna criptomoneda.

Esta posibilidad se indica en último lugar porque no parece lógico que los criminales, que se caracterizan precisamente por la oscuridad en su actividad delictiva, acudieran a un proveedor de servicios registrado, donde aparecerían identificados, para custodiar la criptomoneda obtenida de manera ilícita.

5.3.- ¿CUSTODIA O REALIZACIÓN ANTICIPADA DE LA CRIPTOMONEDA?

Una vez hemos apresada la criptomoneda surge la duda de qué hacer con ella, por lo que pasamos a exponer las alternativas por las que podríamos optar, anticipando que la favorita se considera su realización anticipada, por lo que será la primera a analizar.

El artículo 367 quater de la Lecrim permite la posibilidad de realizar anticipadamente los efectos judiciales de lícito comercio sin esperar a la finalización del pleito. Es la letra d) del párrafo 1 la que podría ser de aplicación en estos supuestos, al amparar la realización anticipada en aquellos casos en que la conservación pueda ocasionar "*una disminución importante de su valor*".

Este riesgo es evidente. El Banco de España y la Comisión Nacional del Mercado de Valores en una nota conjunta publicada el 8 de febrero de 2018, advertían, con relación a las criptomonedas, del elevado riesgo de pérdida de capital invertido que suponen, y también de los problemas de iliquidez y volatilidad extrema que los acompañan.

Se expone lo anterior porque debemos evitar la tentación de mantener en custodia una criptomoneda aprehendida a los delincuentes, bajo el simple pretexto de que pueda aumentar su valor. Los operadores jurídicos, no podemos actuar como entidades especulativas que tengan, entre sus objetivos, el comercializar con los bienes aprehendidos en la búsqueda de un beneficio económico, por lo que debemos huir de dicho atractivo.

Para llevar a cabo esta realización podríamos, previa audiencia de los investigados, bien acudir directamente a un exchanger registrado en España, que nos convirtiese este activo en dinero fiduciario o bien encargar tal cometido a la ORGA. A este respecto hay que indicar que la ORGA carece en el momento actual de protocolo alguno para llevar a cabo esta transacción, aunque ello no supone que puedan llegarla a cabo.

Si optamos por guardar la criptomoneda, el abanico de posibilidades que tenemos es similar al de los delincuentes. Igual que los criminales pueden custodiar sus claves, en un wallet frio o en uno caliente, también nosotros podremos elegir alguna de estas dos alternativas para la guarda de la criptomoneda. Otra posibilidad sería acudir a un proveedor de servicios de custodia.

Exponemos los pros y los contras de cada una de estas opciones.

1.- La custodia en un wallet frío de papel. En este supuesto, la guarda debe corresponder al Laj del juzgado que esté conociendo de las actuaciones. Le correspondería adoptar las medidas necesarias para proteger el wallet en un lugar seguro, alejado de las tentaciones de terceros, pero también, en las condiciones aptas para que el wallet no perdiera la calidad de su impresión.

Tengamos en cuenta que los materiales que disponemos en los juzgados no son los más innovadores, tanto en calidad de papel como tinta, por lo que cualquier desperfecto en el wallet podría ocasionar la pérdida del activo. Pero, además, tampoco las instalaciones de las que gozamos son las óptimas. No son extraños los problemas de humedad y goteras en sede judiciales. También en estos casos si, como consecuencia de cualquiera de estas inclemencias, el wallet donde están las claves sufre un deterioro, el activo sería prácticamente irrecuperable.

Otro problema que pudiera derivarse de la custodia del wallet en el juzgado es que algún tercero, pudiera, en caso de saber dónde se encuentra almacenado, acceder a él y hacer una fotocopia. En este caso las claves estarían en poder de dos usuarios, el juzgado y el tercero, pudiendo este último acceder al activo y hacerse con él.

Por último, si optamos por esta forma de guarda, el wallet debería ser guardado en algún sobre opaco, que impidiera contemplar el interior, y bajo llave en algún cajón del despacho del laj.

Como positivo, al hallarse las claves en un wallet frio, estaría exento de ciberataques.

Como vemos, parecen mayores los problemas de esta custodia que sus beneficios.

2.- Custodia en un wallet frío, tipo hardware. En este supuesto los problemas serán menores que en el *paper wallet*. No hay posibilidad de que se borren números por el mal estado del

papel; ahora bien, no podemos olvidar que el hardware es una especie de usb que deberá ser custodiado bajo llave por el Laj del juzgado. Tendría que evitar, como resulta obvio, su custodia cerca de fuentes de calor o de agua que puedan deteriorar el dispositivo y, con ello, obstaculizar la correcta conservación del bien. También debería guardarse en condiciones tales que eviten el acceso a él por parte de terceros. Al tratarse de un wallet frio, estaría también protegido de posibles ciberataques.

3.- Wallet caliente. El problema más evidente de esta forma de custodia es que la criptomoneda estaría expuesta a ataques informáticos y hackeos, al mantenerse "*on line*" en la red. La tecnología de nuestros dispositivos informáticos no es la mejor ni nuestros equipos disponen de las más modernas medidas de seguridad, por lo que esta forma de custodia no se aconseja en absoluto.

4.- Proveedor de servicios de monederos electrónicos**.** En caso de optar por la conservación de la criptomoneda, y no por su realización, se considera que ésta podría ser una buena opción. El Laj del juzgado no cargaría con la responsabilidad de custodiar el activo, con los riesgos que ya hemos señalado, y quedaría al recaudo de una entidad especializada en la custodia de este tipo de activos.

A este respecto, cabe tener presente que estos proveedores de servicios son sujetos obligados con respecto a la LPBC, y, por lo tanto, en su actividad, deben respetar una serie de obligaciones y garantías que permiten inferir la correcta custodia del activo. Además, dado que esta es su labor y su actividad principal, cabe suponer que tendrán herramientas suficientes para prevenir cualquier ataque informático.

Esta forma de custodia, no obstante, también tiene un par inconvenientes que consideramos menores y que no justificaría acudir a otra vía distinta si optamos por la guarda del activo. En primer lugar, estos proveedores de servicios cobran una tarifa por llevar a cabo su labor. Y, en segundo lugar, éste más preocupante, sería que el *wallet* cerrase su actividad sin previo aviso, en cuyo caso la pérdida podría ser irreparable. Por ello, sería conveniente que la elaboración de algún tipo de protocolo entre la ORGA y/o el Ministerio de Justicia, con algún proveedor de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos, para una custodia mucha más eficiente de las criptomonedas aprehendidas en un procedimiento judicial.

5.4- ¿CÓMO CUANTIFICAR LA RESPONABILIDAD CIVIL Y QUÉ RESTITUIR?

Con relación a la forma en que se puede cuantificar el importe de la responsabilidad, en el caso de mediar criptomonedas dos resoluciones destacan por encima del resto.

En la STS 326/2019, de 20 de junio, el Alto Tribunal opta por indemnizar al perjudicado, no con la devolución de los bitcoins, que era lo que pretendía, sino en la cantidad equivalente al valor de los bitcoins en la fecha de realización de la inversión.

Por el contrario, la SAP de Álava 4/2021, de 15 de enero, elige también la alternativa de indemnizar con dinero, pero, en este caso el importe a indemnizar se calcula sobre la

cotización media que los bitcoins alcanzaron en el período de tiempo en el cual estuvieron sometidos al control del encausado: este criterio fue ratificado por el ATS 109/2022, de 20 de enero.

Las razones del criterio contrapuesto son claras y se fundamentan en las propias características de cada supuesto: mientras que en el caso planteado ante el Tribunal Supremo la cantidad inicialmente entregada era una cantidad monetaria (aunque su finalidad última era que se invirtiese en bitcoins), en el caso planteado ante la Audiencia Provincial de Álava, se trataba criptomoneda cuya venta debió ejecutarse en un periodo de tres días siguientes a su transmisión[23].

Por lo tanto, mientras en el primer caso la cantidad defraudada se fijaría por la cantidad invertida en el momento del acto de disposición patrimonial (con independencia de los dividendos que pudiese dar en futuro), en el segundo caso el perjuicio patrimonial se produciría en función del valor previsible que pudiesen tener los bitcoins durante el período de tiempo en que debieron
ser vendidos (valor que habría operado en detrimento del patrimonio del perjudicado).

En la dirección contraria se encuentra la SAP de Murcia 104/2020, de 14 de julio, donde se decidió por la restitución en la moneda fiduciaria o virtual en que se hubiere realizado la transferencia inicial, apoyándose en los artículos 111 del CP y 1170 del CC y puesto que la transferencia inicial había sido llevada a cabo con bitcoins de igual forma debía efectuarse la restitución.

5.5.- ¿CÓMO RESOLVER EL PROBLEMA SOBRE COMPETENCIA TERRITORIAL O CONFLICTO DE JURISDICCIÓN?

Debemos tener en cuenta que el delito de blanqueo de capitales suele estar estrechamente en relación con la delincuencia organizada y ambas instituciones presentan caracteres similares en cuanto a su carácter transfronterizo. Y si puede afectar a varias jurisdicciones, con más motivo a varios partidos judiciales.

1.- Cabe partir, desde el punto de vista interno, del supuesto de hecho de que los investigados y los perjudicados compartan el mismo partido judicial, con lo que puede surgir un conflicto de competencia territorial, pero también que dada la pluralidad de los investigados, quienes podrían residir en varios puntos de España, la entidad del perjuicio ocasionado, la pluralidad de víctimas en distintas zonas de la geografía española y la dificultad de la investigación, ocasione que el conflicto se dirima entre los órganos territoriales y los órganos centrales.

Tradicionalmente, en nuestros tribunales se aplicaba el principio de ubicuidad para resolver la problemática. Ahora bien, dicho principio ha ido cediendo su protagonismo al de eficacia en la instrucción. Así, el ATS de fecha 20 de diciembre de 2023 acude al principio de eficiencia cuando indica que "*En el caso de estafas informáticas o cometidas a través de Internet o medios similares, empero, esta Sala viene entendiendo que el criterio de ubicuidad, cuando*

[23] ZARAGOZA TEJADA, J.I., "Criptoactivos y criptomonedas. Regulación legal e incidencia en el ámbito penal.", Tratamiento integral del cibercrimen, Formación a distancia del CGPJ, 2022, p. 13-14.

no resulte in casu funcional, ha de ceder en favor de la competencia del Juzgado que esté en mejores condiciones para desarrollar la investigación. Este criterio se aplica cuando se constatan sólidas razones que justifiquen el abandono del criterio competencial ordinario".

También el ATS de fecha 21 de diciembre de 2023, con remisión a otras resoluciones del Alto Tribunal como el Auto del Tribunal Supremo de 18 de diciembre de 2020, Rec. 20220/2020, o de 4 de noviembre de 2021, Rec. 20090/2021, dice: "*Es cierto que la competencia territorial para el conocimiento de los delitos de estafa ha estado tradicionalmente unida a la teoría de la ubicuidad, conforme a la cual, cualquiera de los juzgados que territorialmente estén en disposición de investigar el delito (lugar del desplazamiento patrimonial, lugar de apoderamiento del dinero, lugar de ubicación de las cuentas bancarias...) son competentes para el conocimiento del asunto, optándose por aquel que primero haya comenzado a instruir el procedimiento como criterio de otorgamiento de la competencia. Sin embargo, en los delitos informáticos se desplaza la teoría de la ubicuidad tradicional por el criterio de la eficacia en la instrucción (ver también los AATS de 24/10/19, cuestión de competencia 20389/19, y de 28/11/19, cuestión de competencia 20608/19).*"

Con este criterio de eficacia en la instrucción, establecer qué tribunal será competente va a depender del caso concreto que se esté investigando. En atención a las circunstancias concretas se podrá considerar competente al juzgado del domicilio de los investigados, en otras ocasiones al del domicilio de la mayoría de las víctimas, o al del domicilio del receptador de dinero, o incluso al del lugar donde radiquen los proveedores de servicios o páginas web utilizadas.

2.- También con relación a los conflictos de jurisdicción deberemos acudir al mismo criterio. Así, el Convenio sobre Cibercriminalidad, Budapest, 23 de noviembre de 2001, ratificado por España el día 27 de septiembre de 2010, que en el art. 22.5 establece: "*Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales*"

Como ya se ha esbozado previamente, podemos encontrarnos también con problemas de jurisdicción atendiendo al carácter transnacional del ciberblanqueo de capitales, dentro de cuyas modalidades delictivas se puede incluir el lavado de activos a través de criptomonedas.

El afán de un Estado en investigar y enjuiciar los delitos cometidos en su territorio puede colisionar con el mismo interés de otro Estado, cuando se trate de delitos que se pueden entender cometidos en el territorio de distintos países. Conjugar estos intereses resultará imprescindible, porque el principio "*non bis in idem*" impide que un país pueda imponer su jurisdicción en aquellos casos en los que ya ha actuado la jurisdicción de otro Estado.

Este principio se halla consolidado en el Pacto Internacional de Derechos Civiles y Políticos, en el art. 14.7 al señalar que: "*nadie podrá ser juzgado ni sancionado por un delito por el cual haya sido ya condenado o absuelto por una sentencia firme de acuerdo con la ley y el procedimiento penal de cada país".*

El principio se entiende integrado en el art. 24 de nuestra CE por formar parte del contenido del derecho a la tutela judicial. También se encuentra consagrado en el art. 50 de la Carta de

Derechos Fundamentales de la Unión Europea y en el art. 54 del Convenio de Aplicación del Acuerdo de Schengen.

Por ello será necesario que, cuando un caso de ciberblanqueo afecte a varios Estados y se haya abierto diligencias penales en más de un país, las respectivas autoridades deberán llegar a un pacto ya sea para unificar el procedimiento o en supuestos especiales para establecer lo que se ha de perseguir y enjuiciar en cada uno de ellos, garantizando el respeto del "*no bis in idem",* pudiéndose incluso constituir, para ello, un equipo conjunto de investigación entre los países afectados, a los efectos de alcanzar el mejor acuerdo posible en el éxito de la investigación.

Para facilitar estos acuerdos el convenio sobre cibercriminalidad, en el art. 22.5, antes expuesto, establece que los Estados celebraran consultas buscando cual es la jurisdicción que se encuentra en mejor situación para llevar a cabo la persecución eficaz de los delitos.

BIBLIOGRAFÍA

BLANCO CORDERO, I. "El delito de blanqueo de capitales", Aranzadi, Cizur Menor, 2022, p. 31.

CASANUEVA CAÑETE, D. y LÓPEZ DE LA CRUZ, N., "*El concepto de criptomoneda y breves consideraciones en torno a su tributación", p.* 79-80

CEDIEL A., y PÉREZ POMBO E.A., "Fiscalidad de Bitcoin, monedas virtuales y tokens", Editorial Atelier, 2023, pp 15-16.

FISCALÍA GENERAL DEL ESTADO. Circular 4/2010 sobre las funciones del Fiscal en la investigación patrimonial en el ámbito del proceso penal.

GÓMEZ INIESTA, D.J., "Utilización de las nuevas tecnologías en la comisión del blanqueo de dinero", en ABEL SOUTO, M., y SÁNCHEZ STEWART, N. V Congreso sobre Prevención y Represión del Blanqueo de Dinero: Ponencias y conclusiones del congreso sobre las reformas de 2015 e incidencia en la economía y sociedad digital, Tirant lo blach Online, 2018.

GUDÍN RODRÍGUEZ-MAGARIÑOS, F., Criptoactivos: de la paralegalidad a la paulatina legalización, Editorial Jurídica Sepin, Madrid, 2022.

JUEGA CUESTA, J., Criptoactivos y monedas virtuales: marco regulatorio y tributación, Editorial Lefebvre-El Derecho, S.A., Madrid, 2023.

MUÑOZ MACHADO, S. "La regulación de la red. Poder y derecho en internet, Editorial Taurus, Madrid, 2000

NAKAMOTO, S. "Bitcoin: Un Sistema de Efectivo Electrónico Usuario a usuario", https/bicoin.org/files/bitcoin-paper/bitcoin_es_latam.

NAVAS NAVARRO, S., "Un mercado financiero floreciente: el del dinero virtual no regulado (Especial atención a los Bitcoins)" *Revista CESCO de Derecho de Consumo*, n.º 13, 2015, pág. 90.

PEDREIRA MENÉNDEZ, J., *"La contabilización y tributación de la moneda digital (Bitcoins)"* IEF, Documentos de trabajo 20/2018 (1.ª parte), pág. 144

PÉREZ BERNABEU, B., "La administración tributaria frente al anonimato de las criptomonedas: la seudonimia del Bicoin", *Documentos-Instituto de Estudios Fiscales*, nº10, 2018, pag 150.

PÉREZ LÓPEZ X., "Las criptomonedas: consideraciones generales y empleo de las criptomonedas con findes de blanqueo", FERNÁNDEZ BERMEJO, D., Blanqueo de capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas, Editorial Aranzadi SAU, Navarra, 2022, p. 94-97

PÉREZ LÓPEZ, X., “El blanqueo de capitales a través de las criptomonedas”, SANZ DELGADO E. y FERNÁNDEZ BERMEJO D., *Tratado de Delincuencia Cibernética,* Aranzadi SAU, Navarra, 2021, p 542.

TAÚS BALLESTER, J.J., “La responsabilidad penal de los wallets y los Exchange dentro del delito de blanqueo de capitales”, Diario La Ley, número 10346 de 12 de septiembre de 2023.

ZARAGOZA TEJADA, J.I., “Criptoactivos y criptomonedas. Regulación legal e incidencia en el ámbito penal.”, Tratamiento integral del cibercrimen, Formación a distancia del CGPJ, 2022, p. 13-14.