Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Derecho Penal Económico

El uso de criptoactivos como nuevo método comisivo de blanqueo de capitales.

Trabajo de fin de estudios presentado por:	Ana Verdeguer Crespo
Tipo de trabajo:	Trabajo de Fin de Máster
Director:	Dr. Alembert Vera Rivera
Fecha:	22/09/2022

Resumen

El presente trabajo está dirigido a investigar los métodos «emergentes» de blanqueo de capitales; esto es, la manera en la que el avance de las nuevas tecnologías influye en el surgimiento de nuevas maneras a través de las que los ciberdelincuentes pueden llevar a cabo su actividad ilícita. Para favorecer el desarrollo de la argumentación, esta se centrará en los distintos usos fraudulentos de los criptoactivos para blanquear capitales, aunque también tratará otras cuestiones jurídicas de relevancia. Además, se hará especial mención a la Directiva (UE) 2018/843, por las importantes modificaciones que incorpora con respecto a la lucha contra el lavado de dinero y el inicio de una regulación preventiva frente a la utilización delictiva de los criptoactivos para tal fin.

PALABRAS CLAVE: Blanqueo de capitales, criptoactivos, cadena de bloques, anonimato, trazabilidad.

Abstract

The current work investigates money laundering "emergent" methods; meaning, the way new technologies' advancement influences the emergence of brand-new forms for cybercriminals to continue carrying out their illicit activity. To favor the argument's development, it will focus on the different fraudulent uses of cryptocurrencies to launder money, although it will also deal with another relevant legal issues. In addition, special mention will be made about Directive (EU) 2018/843, due to the important modifications that it has incorporated, regarded to the fight against money laundering and the beginning of a preventive regulation against the criminal use of crypto assets for this exact purpose.

KEY WORDS: laundering money, crypto assets, Blockchain, anonymity, traceability.

Índice de contenidos.

I. INTRODUCCIÓN.

El presente trabajo desarrollará un análisis jurídico y político-criminal acerca de la proliferación y métodos del uso fraudulento de los criptoactivos para blanquear dinero, ello a causa de las nuevas posibilidades que ofrece el sinfín de avances tecnológicos que venimos experimentando en las últimas décadas y, con ello, la consiguiente modernización del Derecho Penal.

A tal efecto, se va a confeccionar en primer lugar una conceptualización independiente y autónoma del blanqueo de capitales y los criptoactivos, que haga la función de guía con la intención de facilitar el seguimiento de la mecánica adoptada en los epígrafes subsiguientes. Al estar pensado para que ejerza meramente de prolegómenos, no se profundizará en exceso pero tampoco pasarán desapercibidos aspectos que aún suscitan debate entre la doctrina científica y que son elementos esenciales a considerar cuando se habla de blanqueo de capitales —problemática referida al bien jurídico protegido, al objeto material o al delito antecedente— o de criptoactivos —su naturaleza jurídica, su relevancia en el ámbito penal y económico o los nuevos indicadores de riesgo que derivan de su existencia—.

Seguidamente, se abrirá el capítulo que circunscribe el tema central de la investigación: La mención y correspondiente análisis de algunas de las modalidades más habituales en tiempos recientes de blanqueo de capitales a través del uso de criptoactivos. Se verán, ilustrativamente, casos actuales de prensa que escenifiquen las comisiones propuestas; la compraventa de criptomonedas o el *smurfing,* como técnicas más frecuentes.

Como último —pero no menos importante— punto, se apreciarán cuestiones «controvertidas» de carácter jurídico, nacidas a raíz de la naturaleza del propio sistema de codificación de la cadena de bloques *(blockchain)*: Cómo el anonimato que esta proporciona, así como la dificultad de la trazabilidad de operaciones, pondrán absolutas trabas en la investigación de las mencionadas modalidades. De este modo, se va a abordar la problemática de la determinación del tribunal competente. También se hablará, por su parte, del papel del decomiso penal en estas situaciones.

En los apartados venideros se dará una mayor aproximación de la manera en la que se ha configurado el trabajo, con el fin de aportar una visión panorámica tanto de su naturaleza como del contenido que ofrece.

1. Justificación del tema elegido.

El lavado de activos es una práctica comúnmente conocida y extendida, y los métodos habituales no escapan del conocimiento general; se puede desconocer la técnica, la jerga jurídica o la legislación al respecto, pero se sabe cómo funciona y cuáles son los resultados. No obstante, los avances tecnológicos han ofrecido, en términos generales, tantas facilidades como complicaciones y ese es el eje entorno al cual virará el proyecto: La manera en la que el progreso de la informática y la tecnología puede llegar a incidir en la gestación de nuevas técnicas de comisión de delitos, utilizando de una mano el delito de blanqueo de capitales y de otra los criptoactivos para poder elucidar la cuestión minuciosamente.

Así pues, se encontrará en todo momento en el punto de mira un comportamiento delictivo con particular y dilatado recorrido histórico, pero sobre el cual se vienen esgrimiendo métodos innovadores que han traído consigo ciertas complicaciones criminógenas, procesales y penales y que, por su carácter novedoso, aún requieren profundización en la tarea analítica, del mismo modo que aún provocan división doctrinal y —no excesivamente pacífico— debate jurídico. Algo, por otra parte, necesario para empezar a dar respuestas fundadas y efectivas para estos nuevos desafíos.

Ello conformará, en conclusión, el motivo por el cual se va a realizar el estudio sobre «El uso de criptoactivos como nuevo método comisivo de blanqueo de capitales».

2. Problema y finalidad del trabajo.

Como bien se ha expuesto en el apartado anterior, los avances tecnológicos han influido consistentemente en la dinámica habitual de comisión de delitos, propiciando la creación de innovadoras formas de llevarlos a cabo por parte de los delincuentes y, en concreto, de los

informático-económicos. El problema surge cuando este tipo de perfiles criminales aprovecha las posibilidades que la digitalización ofrece para sus fines delictivos, pues se mueven en un terreno que todavía no ha sido objeto de legislación y que, por su carácter novedoso, tampoco se conoce en exceso.

Se obstaculiza, pues, la tarea de aplacar la criminalidad económica, especialmente aquella de mayor gravedad —como es el blanqueo de capitales—, cuando los ciberdelincuentes aprovechan las ventajas de la criptografía para delinquir. Caracteres beneficiosos como el elevado índice de privacidad y anonimato o la opacidad de la trazabilidad de las transacciones no solo complican la labor investigadora, sino que también plantea serias cuestiones a nivel jurídico a las que aún no se les ha ofrecido una respuesta sólida, unitaria.

Esa será la problemática inicial desde la cual se parte en el presente trabajo, teniendo como finalidad arrojar claridad al asunto para diluir la controversia que este uso delictivo de los criptoactivos está generando en la actualidad, así como comprender cómo opera en la praxis el cibercriminal que hace uso de estas nuevas técnicas y, por último, analizar las cuestiones jurídicas transcendentes surgidas a raíz de esta coyuntura.

Todo ello llevará inevitablemente a una conclusión final que, —adelantamos—, se dirigirá hacia el peso y la eficacia de la prevención frente a todo tipo de delincuencia.

3. Objetivos.

Con el fin —y la esperanza— de contribuir al estudio de estas nuevas técnicas comisivas, y para poder realizar este trabajo con el rigor y la claridad que requiere, se ha establecido una relación cerrada de objetivos a alcanzar durante y a la finalización del estudio, siendo estos:

1. Dominar la teoría jurídica del delito de blanqueo de capitales y su relación con métodos comisivos emergentes a raíz de los avances tecnológicos.
2. Contribuir al debate que de por sí suscita la existencia de medios digitales criptográficos de intercambio y su utilización con fines delictivos.
3. Tener la capacidad de generar un ensayo jurídico-crítico constructivo respecto a fenómenos que son de actualidad.

4. Valorar con criterio la normativa existente y realizar propuestas de prevención de semejante tipología de delitos, todo ello desde un enfoque puramente jurídico.
5. Evaluar cuestiones jurídicas controvertidas a las que el Derecho todavía no ha dado una respuesta unitaria.

A la finalización del proyecto, se pretende haber alcanzado un alto grado de conocimientos en la materia, con el fin de poder formular conclusiones que respondan a los objetivos mentados y, del mismo modo, resolver las diferentes hipótesis que hayan surgido a raíz de estos a lo largo de la investigación.

II. EL BLANQUEO DE CAPITALES Y LOS CRIPTOACTIVOS: CONSIDERACIONES PREVIAS.

En la actualidad, los delincuentes económicos encuentran cada vez más dificultades a la hora de sacar provecho de las ganancias derivadas de su actividad delictiva y, sobre todo, a la hora de dotarles de apariencia legal, en especial porque las autoridades judiciales y policiales conocen de sobra los diferentes *modus operandi* y, hasta no hace demasiado, tenían descifrados los patrones operativos de estos perfiles de criminales. El imparable avance de las nuevas tecnologías les ha permitido desarrollar técnicas mucho más complejas que sí escapan del conocimiento de las referidas autoridades, precisamente por su carácter novedoso y por su amplia extensión de posibilidades, por lo que ha resultado necesaria la intervención de la ciencia criminógena para estudiar y delimitar estos nuevos métodos, con el fin de poder atajarlos y prevenirlos.

Con todo, es consenso ratificado por el total de la doctrina científica que el riesgo de que los criptoactivos sean utilizados por los criminales para el lavado de dinero es cierto y es, además, elevado; como veremos, las propias características de los criptoactivos propugnarán su uso como herramienta «lavadora» de dinero.

Para poder llegar a esa conclusión, parece necesario realizar primero una precisión independiente de ambos conceptos: Por un lado, se refrescarán los aspectos más relevantes que rodean al delito de blanqueo de capitales; por otro, se ofrecerán unas primeras pinceladas respecto al «criptoactivo» y su entorno, con el fin de que sirva de guía de cara a la posterior exposición del tema.

A. Aproximación a la teoría jurídica del blanqueo de capitales.

El blanqueo de capitales comprende aquellas conductas realizadas con intención de incorporar al tráfico económico legal bienes y ganancias derivados de conductas delictivas previas, de modo que puedan ser usados y disfrutados al otorgársele apariencia de legalidad.

Interesa al Derecho Penal por la magnitud de la actividad blanqueadora en la práctica, por el grave impacto que produce en nuestra economía, por la distorsión de la carga tributaria que estas ganancias deberían de soportar… Según MUÑOZ CUESTA (2013, citado en FERNÁNDEZ BERMEJO, 2016, p. 213), puede «dar lugar a una desestabilización de las condiciones del mercado y la competencia», atentando «a la estabilidad y al buen orden del mercado financiero».

No obstante, para algunos como SILVA SÁNCHEZ (2011, p. 133), la inclusión del blanqueo de capitales como precepto independiente no es sino «una manifestación paradigmática del proceso de expansión del Derecho penal». Algunos autores se refieren a esto último como «la creación de delitos nuevos, la imposición de penas cada vez más severas y la búsqueda de una mayor eficacia —obviamente, represiva— frente a la criminalidad» (LANDROVE DÍAZ, 2010, p. 54). El recrudecimiento penal que describe el autor es, de hecho, el gran sesgo que se está viviendo en la praxis político-criminal: Un importante sector de la doctrina científica considera que el discurso del riesgo, asentado en la sociedad y con base en los supuestamente elevados niveles de criminalidad, está provocando un afán regulatorio desmedido, incoherente con respecto a nuestros preceptos constitucionales, y resultante en la generación de normativa ineficaz, cuestionablemente paliativa y escasamente resolutiva.

Como fuera, y con independencia de la división doctrinal al respecto de la más reciente estipulación normativa, se hará una breve representación de los puntos clave de la regulación vigente, empezando por su delimitación terminológica y funcional.

1. Definición, fundamentación y concreción de sus fases.

El blanqueo de capitales es comúnmente definido como un delito contra el patrimonio y el orden socioeconómico, cuyo objetivo es integrar en el tráfico económico-jurídico bienes o ganancias de procedencia ilícita. Las conductas que se realizan con dicho fin persiguen dotar de apariencia de legalidad a sendos bienes, borrando así el rastro de ese origen delictivo.

Aparece reflejado de esta manera en la STS 265/2015, de 29 de abril, cuando el Ponente Excmo. Sr. D. Cándido Conde Pumpido Tourón describe que «el Código Penal sanciona como blanqueo de capitales aquellas conductas que tienden a incorporar al tráfico legal los bienes, dinero y ganancias obtenidas en la realización de actividades delictivas, de manera que,

superado el proceso de lavado de los activos, se pueda disfrutar jurídicamente de ellos sin ser sancionado».

Esos comportamientos mencionados son enumerados por el legislador en su propia redacción del artículo 301 del Código Penal español (en adelante, CP), ubicación en la que se encuentra tipificado el blanqueo de capitales. De esta forma, se está tratando de blindar los circuitos del dinero, de modo que una actividad delictiva no pueda considerarse, en suma, un recurso rentable para los delincuentes económicos. Esta es la fundamentación principal de la regulación penal del lavado de dinero: Evitar el aprovechamiento económico de los delitos.

También es jurisprudencia de la Sala Segunda del Tribunal Supremo que «la razón de política criminal de estos tipos delictivos es evitar que los autores de delitos logren la incorporación al tráfico económico legal, de los bienes, dinero, ganancias y beneficios procedentes de sus actividades delictivas». Esta cita pertenece al Fundamento de Derecho decimocuarto de la STS 1080/2010. En efecto, la idea principal es que estos beneficios obtenidos a raíz de la comisión de un delito no se incorporen al sistema económico legal. Y esto puede interpretarse desde distintos puntos: por un lado, se pretende anular ese incentivo que puede suponer para el delincuente económico disfrutar de aquello que gana al cometer un delito. Por otro, se desea minimizar el riesgo de impacto o repercusión que este tipo de conductas delictivas puede tener en la propia construcción económica de la sociedad.

En cuanto a la actividad blanqueadora, esta no consiste en hechos puntuales, aislados; se trata en realidad de una secuencia de actos o fases. Así, de acuerdo con la doctrina establecida por el Grupo de Acción Financiera Internacional (en adelante, GAFI), las etapas del blanqueo serían las siguientes:

1ª) *Placement* o colocación.

En esta primera fase de introducción, el blanqueador intenta hacer desaparecer el origen ilícito del dinero, o al menos desligarlo de los bienes o ganancias obtenidos. Es, sin lugar a duda, un paso arriesgado; en términos generales, se trata de cantidades considerables de dinero —normalmente, efectivo— y no es en absoluto sencillo introducirlas, así como así, en el tráfico económico-jurídico.

Uno de los métodos con más presencia en la actualidad consiste en ir realizando ingresos en cantidades pequeñas, dosis insignificantes para las entidades bancarias que pueden no

levantar sospechas y que, además, no conllevan la identificación de la persona que está efectuando el depósito. Es la técnica conocida como *pitufeo* o *smurfing*, que será explicada con mayor detalle en posteriores epígrafes. No obstante, y como materia que nos ocupa, otra vía muy recurrida por los blanqueadores para llevar a cabo el *placement* será la utilización de monedas virtuales, casos que también estudiaremos más detenidamente en el siguiente capítulo.

2ª) *Layering* o diversificación.

Una vez introducido en el sistema financiero, la segunda etapa del blanqueo requiere que ese dinero o esos bienes se desliguen lo máximo posible de su fuente de origen. El blanqueador, en este momento del proceso que ha iniciado, necesita ir borrando el rastro que haya podido dejar en su primera operación de colocación, realizando numerosos movimientos destinados a ese fin encubridor. Por ejemplo, los activos podrían ser enviados mediante transacción bancaria a distintas sucursales de una misma entidad.

3ª) *Integration* o integración.

Lograda la apariencia legal, el blanqueador necesita que esa «dotación» sea totalmente efectiva. Es decir, poder utilizar legalmente los bienes o ganancias transformados en la fase anterior. Así, quedará constancia de su utilización en registros contables y tributarios, llegando a su completa integración en el tráfico jurídico.

Antes de terminar el presente apartado, cabe dedicar un espacio concreto a aludir la figura del antes citado GAFI, dada su importancia a nivel internacional y, en especial, en la materia que nos ocupa: Se trata de un ente intergubernamental que lleva operando desde el año 1989, y cuya actividad principal se dirige a la toma e implantación de medidas y protocolos para combatir el blanqueo de capitales, la financiación del terrorismo y la proliferación de armas de destrucción masiva. Sus directrices, aunque no vinculantes, se han convertido a nivel global en verdaderos estándares para la Unión Europea y para los propios Estados.

Destacan, en este sentido, las denominadas «40 recomendaciones del GAFI», considerado el marco básico de combate del blanqueo de capitales. Constituyen, sin lugar a duda, sus estándares internacionales más reconocidos, y reúnen una serie de medidas de carácter legal, financiero, conductuales y de cumplimiento; adoptadas eficazmente por los

países, no solo se contribuiría a aumentar la transparencia, sino que también permitiría que ellos mismos pudieran implementar medidas y llevar a cabo acciones destinadas a proteger sus sistemas financieros de un posible uso fraudulento.

A lo largo del proyecto se mencionará repetidamente por su sólido rol en la persecución de estos delitos, y cuya actividad coincide de pleno con la materia que nos ocupa en este trabajo, de ahí que se haya abierto un breve inciso para otorgarle, inicialmente, una definición y un contexto.

2. Cuestiones referidas al bien jurídico protegido y al objeto material del delito.

La especificación del bien jurídico que se protege al tipificar el blanqueo de capitales ha sido notablemente discutida, debate que se pretende plasmar lacónicamente en este epígrafe al ser una cuestión relevante pero que no integra el núcleo del proyecto.

En un primer lugar, la gran «discusión» nace con la inclusión de un tipo penal denominado «blanqueo de capitales», de contenido análogo a un delito preexistente conocido como el delito de receptación. El delito de receptación se perfecciona cuando un individuo presta ayuda a los autores materiales de un delito para que puedan utilizar y disfrutar los efectos derivados de la conducta delictiva previa, mediando ánimo de lucro.

En efecto, nos parece que estos comportamientos y los descritos en el tipo del blanqueo son subsumibles entre ellas: como bien señala CALDERÓN TELLO (2017, p. 324), «la prohibición […] es la misma, con diferentes ámbitos de aplicación. […] Lo que estos tipos penales protegen es lo mismo». Entonces, ¿existe, a todos los efectos, un solapamiento? Lo cierto es que, en la actualidad, se presentan como delitos totalmente autónomos.

Para lograr una diferenciación de lo que se considera que protege, según la doctrina, el blanqueo de capitales, se van a delimitar las distintas teorías que se han propuesto a lo largo de los años al respecto:

1ª) La primera teoría formada sobre el bien jurídico protegido en el delito de blanqueo de capitales entendía que este coincidía con el bien jurídico protegido del delito anterior. Es decir, no tendría uno propio, sino que el bien que se lesiona con la actividad delictiva previa

es el que nuevamente se estaría lesionando con el blanqueo. Probablemente se encuentre, en la propia temática, de entre las teorías más criticadas por su argumentación:

Para mayor concreción, quienes se muestran favorables a esta posición doctrinal entienden que «la conducta no se agota en el resultado del delito previo, sino que continúa con las conductas de blanqueo de capitales […] La conducta del delito de blanqueo de capitales es parte del delito previo considerado como un paso posterior y necesario a la comisión del delito del cual se obtienen los bienes a blanquear o legitimar» (CALDERÓN TELLO, 2017, p. 362).

A simple vista, parece que esta postura no se corresponde con la supuesta intención del legislador de crear un delito autónomo, ya que esta interpretación claramente aboga por una dependencia del delito inmediatamente anterior que no dejaría posibilidad alguna de que el blanqueo de capitales se configurase como independiente. Y, como decíamos, no encaja en la redacción que se le ha dado al artículo 301 del Código Penal, por lo que no parece que pudiera tener encaje como fundamentación aislada para configurar el bien jurídico protegido en este delito.

2ª) La segunda teoría incluye a la Administración de Justicia como bien jurídico protegido, en el sentido de que las conductas que se llevan a cabo para cubrir el rastro delictivo de los bienes y ganancias obstaculizan, en sumo grado, la investigación y persecución del primer delito cometido.

En este sentido, la doctrina no se refiere a la Administración de Justicia como institución, sino que las pretensiones de amparo se centran en su correcto funcionamiento. Se trata de otra teoría ampliamente debatida:

Los argumentos a favor de esta posición residen en el carácter encubridor de las conductas blanqueadoras: de igual modo que el delito de encubrimiento (artículos 451 a 454 CP) tutela el correcto funcionamiento de la Administración de Justicia, la tipificación del blanqueo de capitales debería coincidir en cuanto al bien jurídico que pretende proteger, en base a la naturaleza de las conductas descritas. Así, se entendería que la conducta típica del blanqueo «se encuentra más cerca del encubrimiento que de las conductas receptadoras» (CALDERÓN TELLO, 2017, p. 357).

Lo cierto es que, si bien es cierto que las conductas típicas del blanqueo de capitales conllevan evitar el descubrimiento de la identidad del autor o autores materiales del delito

principal, no parece ser este el motivo por el cual nace este tipo penal. Esto viene a significar que, si el correcto funcionamiento de la Administración de Justicia fuese el único bien jurídico que tutelar, se estaría dejando de lado, entre otras muchas cosas, uno de los elementos más significativos que derivan de estos comportamientos: Que los efectos resultantes del delito antecedente no «contaminen» el tráfico económico.

Es decir, es evidente que estas conductas perjudican, bien sea directa o indirectamente, al funcionamiento de la Administración de Justicia, pero la realidad es que no se puede considerar que esta sea la verdadera razón de ser del blanqueo de capitales. Por ende, se necesita una construcción mucho más compleja en cuanto al bien jurídico protegido.

3ª) El orden socioeconómico como bien a proteger jurídicamente también aparece como posibilidad, y es comprensible que así se considere, entre otros motivos, por la ubicación que ostenta en el Código Penal español, formando parte del Título XIII cuya rúbrica es «Delitos contra el patrimonio y contra el orden socioeconómico».

Como bien entiende CALDERÓN TELLO (2017, p. 355), «la circulación de los bienes legales en la economía debe ser protegida contra la contaminación que supone el hecho de la incorporación de los bienes de procedencia delictiva»; DEL CARPIO DELGADO (1997, p. 82, citado en CALDERÓN TELLO, 2017, p. 355) lo asimila como el fundamento del blanqueo de capitales. Como decíamos antes, este es uno de los elementos esenciales en cuanto a las conductas típicas descritas, o mejor, en cuanto a la toma de decisiones acerca de cuál debe ser el bien jurídico tutelado. Algunos incluso lo tomarán como la respuesta idónea para la controversia planteada al respecto, como veremos más adelante.

4ª) El blanqueo de capitales como delito pluriofensivo: En efecto, cabe la opción de que no se proteja un solo bien jurídico, sino que sean varios los que se pretende tutelar. Es esta tesis la seguida por un amplio sector jurisprudencial. En este sentido, la STS 1013/2014: «se suele convenir en que se trata el de referencia de un delito pluriofensivo, en cuanto que ataca el orden socioeconómico, a la Administración de Justicia y también al bien jurídico protegido por el delito subyacente».

A esto veníamos a referirnos al establecer que este tipo de conductas requerían de una «construcción mucho más compleja». Admitir la cualidad de pluriofensividad va a permitir que

se pueda proteger más de un bien jurídico; relacionados, podrían dar respuesta al resultado que se prohíbe en este tipo penal (CALDERÓN TELLO, 2017, p. 360). Se trataría, pues, de una suma de los aspectos antes adjudicados como «correctos, pero autónomamente insuficientes». Si hay algo en lo que mayormente coincide la doctrina científica es que el legislador ha impuesto una pena severa para estas conductas, lo que de algún modo puede enlazarse con la gravedad de los comportamientos y la variedad de bienes jurídicos protegidos a los que afecta.

Es interesante, a este respecto, el punto de vista del autor que se ha citado reiteradamente para la exposición de este apartado: Contrariamente al sentido jurisprudencial, CALDERÓN TELLO (2017, p. 369) expone en su tesis su rechazo hacia el carácter pluriofensivo del bien jurídico protegido en el blanqueo de capitales, fundamentándolo en el hecho de que la protección mediata «no es el objeto de la prohibición de blanquear, aunque sean esperables y deseables». Encuentra, así, que el bien jurídico tutelado únicamente es el «tráfico lícito de bienes», afectado como bien inmediato.

Por lo que se refiere al objeto material, se ha de atender a la redacción del precepto: Este conviene que serán «bienes» cuyo origen se encuentre en una actividad delictiva que, en cualquier caso, será previa a la conducta típica del blanqueo. De acuerdo con la Directiva 2005/60/CE, «bien» puede ser «todo tipo de activos, tanto materiales como inmateriales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluidas la electrónica o la digital, que acrediten la propiedad de dichos activos o un derecho sobre los mismos». Así, para el blanqueo de capitales el objeto material se traducirá en «los bienes en que se tradujeron las ganancias del delito» (ROMERO FLORES, 2002).

Los bienes «integran el elemento de la estructura típica en torno al que orbitan todos los demás» (CALDERÓN TELLO, 2017, p. 407). Lo cierto es que la interpretación que se le ha venido dando al concepto de bienes que ofrece el artículo 301 del Código Penal puede enmarcarse en el ámbito del alzamiento de bienes, de modo que encarta la definición dada por la Directiva 2005/60/CE, antes citada. En resumidas cuentas, «bienes» como expresión podría incluir cualquier tipo de beneficio, siempre que represente «un incremento patrimonial y que es valorable económicamente» (MUÑOZ CONDE, 2002, pág. 358, citado en CALDERÓN TELLO, 2017, p. 412). Esta definición, en sentido meridianamente amplio, se corresponde con

el sentir europeo, que decidió acertadamente renunciar a limitar el objeto material del delito y separarse de una concepción estricta, para poder encajar más adecuadamente a las conductas todas las formas de blanquear que existen y que han ido modernizándose con los años. Es fácilmente apreciable, pues, que la redacción vigente del precepto de blanqueo da cabida a técnicas nuevas para cometerlo, pudiendo incluir entonces aquellas que trataremos en el presente trabajo: los criptoactivos.

3. El delito previo.

La actividad ilícita antecedente es el presupuesto base o habilitante del blanqueo de capitales, pues sin ella no habría constructo legal posible. De la redacción del precepto se extrae la necesidad de que exista un comportamiento delictivo previo. Parece llano y sencillo, pero la doctrina ha adoptado dos posiciones distintas al respecto: Un sector opina que la circunstancia del delito previo es un elemento normativo del tipo, y existe otra parte que considera que es una condición objetiva de punibilidad.

Hay novedades reseñables al respecto y es que jurisprudencia reciente ha aceptado que pudiera no ser absolutamente precisa la existencia de una sentencia firme condenatoria por esa conducta anterior. Ejemplo de ello es la STS 9965/2001, siendo palabras del magistrado Cándido Conde-Pumpido Tourón: «basta con la conciencia de la anormalidad de la operación a realizar y la razonable inferencia de que procede de un delito grave». Inmediatamente, surgen las siguientes incógnitas: ¿Cómo es ello posible, si no hay resolución en firme que constate que la acción ha sido, en efecto, delictiva? ¿Esta asunción no estaría colisionando frontalmente contra la presunción de inocencia? Bien, en este sentido entra en juego la conocida como prueba indiciaria o circunstancial. Para ilustrar cómo opera esta valoración de la prueba en el proceso penal se utilizará la STS 3504/2019, interesantísima y completamente didáctica resolución en la que el magistrado Vicente Magro valoró la suficiencia de una considerable suma de indicios para fallar contra los acusados.

Que este supuesto exista y tenga cabida en la realidad no es sino por la gran cantidad de casos en los que, en la práctica, no ha sido ni es posible hallar pruebas directas. Tal y como aparece reflejado en la sentencia citada, la doctrina científica define la prueba indiciaria como

«la suma enlazada y no desvirtuada de una serie de datos; datos base, que a través de ellos, permiten al Juez arribar el hecho consecuencia por medio de un explícito juicio de inferencia fundado en un razonamiento lógico-inductivo en el que la solidez de los indicios avalan la solidez de la conclusión, siempre en los términos propios de la certeza judicial y que se puede concretar en la fórmula sacramental que emplea el Tribunal Europeo de Derechos Humanos; *certeza más allá de toda duda razonable*» (Fundamento de Derecho SEGUNDO, STS 3504/2019).

En otras palabras —en las de la propia Sala, concretamente—, se trata de una «concatenación y unión de indicios que por sí solos no servirían para condenar, pero sí la suma de ellos», que es lo que lleva al Tribunal «a la convicción de la autoría». En la misma sentencia se fijan ni más ni menos que veinte criterios, de carácter orientativo, que podrían servir para considerar suficientes dichos indicios en situaciones de ausencia de prueba directa. A fin de cuentas, será necesario que la actividad delictiva antecedente quede perfectamente relacionada.

B. Aparición de los criptoactivos en el panorama socioeconómico actual.

Durante las dos últimas décadas hemos visto cómo se ha introducido en nuestro vocabulario una nueva terminología, consecuencia de las últimas innovaciones tecnológicas que han permitido digitalizar activos físicos como, por ejemplo, el dinero.

En 2009 emergió la tendencia de las criptomonedas. Durante los primeros años, todo lo que se conocía era *Bitcoin*; casi veinte años después, son innumerables las categorías existentes, de tal manera que se han terminado por agrupar —tal y como explicaremos en los siguientes apartados— en dos grandes grupos: criptomonedas y *tokens*.

Que este tipo de tecnología estuviese a disposición del usuario era cuestión de tiempo, ahora existe la posibilidad de realizar operaciones y transacciones sin que las entidades financieras tengan facultad de intervención, punto que, no es de extrañar, resulta cuantiosamente atrayente, en especial para aquellos que busquen beneficiarse de las ventajas que la codificación de la cadena de bloques ofrece: Anonimato y dificultad de trazabilidad de los movimientos, una combinación más que provechosa para esta categoría de delincuentes económicos.

Así, en los posteriores epígrafes, se va a realizar un análisis superficial de los activos criptográficos para facilitar la comprensión del término y su funcionamiento, además de ofrecer una explicación somera de cómo se les puede dar —y se les da— un uso delictivo y qué espacio ocupa o debería ocupar en el plano jurídico-penal. Todo ello a modo de prolegómenos.

1. Descripción del término, tipología y funcionamiento.

Aunque este sea un tema de rigurosa actualidad, no todo el mundo conoce todavía el funcionamiento del mundo criptográfico, o qué son exactamente las divisas o activos virtuales. Para ello se albergará este espacio, de modo que pueda servir como guía previa.

En primer lugar, se puede definir «criptoactivo» como la «representación digital de valores o derechos susceptibles de negociación y archivo electrónico mediante el uso de tecnología que permite el registro distribuido de datos cifrados u otra similar» (DE MIGUEL ASENSIO, 2020, p. 2). Sería necesario convenir en este punto que criptoactivo no es sinónimo de criptomoneda; la segunda forma parte de aquello primero, siendo este un concepto infinitamente más amplio y que, como se ha mencionado previamente, incluye otro tipo de figuras digitales como, por ejemplo, el *token* o ficha.

Explicar el funcionamiento de manera llana y taxativa es, sin duda, tarea ardua ya que implica inexorablemente el uso de terminología técnica. La cadena de bloques es un tipo de sistema «DLT», que en resumidas cuentas es un sistema de registros distribuidos. En otras palabras, es «tecnología de almacenaje de datos de la que existen múltiples copias idénticas distribuidas entre aquellas personas que participan en la red» (ROMERO UGARTE, 2018, citado en PÉREZ-MEDINA, 2020, p. 3). Siguiendo la línea de definición, VEINTEMILLA CANDO (2022, p. 14, citando a TAPSCOTT, A; TAPSCOTT, D, 2016) interpreta la cadena de bloques como «un libro de contabilidad digital incorruptible de transacciones económicas que se puede programar para registrar no solo transacciones financieras, sino prácticamente todo lo que tiene valor». Se trata, pues, de tecnología avanzada, gracias a la cual se pueden llevar a cabo operaciones —digitales— seguras, descentralizadas, sincronizadas y distribuidas.

Los criptoactivos se dividen en dos grandes grupos, siendo las criptomonedas y los tokens:

1º) Las criptomonedas son medios digitales de intercambio, cifradas criptográficamente para blindar su titularidad. En definitiva, son monedas que no existen físicamente, y habitualmente se suelen guardar en *e-wallets* o carteras, también digitales. El ejemplo que todos conocemos es el *Bitcoin,* aunque con el paso de los años han ido surgiendo nuevos sistemas de pago (*Ethereum, Cardano, Tether…).*

2º) Por su lado, los tokens son definidos (MOUGAYAR, 2016, citado en GARCÍA BERNÁRDEZ, 2017) como «una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas». Son, en definitiva, unidades de valor cuya operatividad reside en la criptografía y que son emitidas por entidades privadas, con funcionalidades similares a la prestación de un servicio.

Podrían ser utilizados, por ejemplo, para dar una prestación a cambio de un trabajo realizado, pero la realidad es que pueden tener la utilidad que la persona u organización que lo haya creado y desarrollado desee. Es una tecnología algo más compleja que la criptodivisa, todavía no hay una construcción sólida al respecto, pero, aún así, los NFT están ganando cada vez más presencia en el día a día. Es más, los hay que empiezan a considerar que el volumen de negocio de los NFT está creciendo, contrariamente al mercado de las criptomonedas, que no solo lleva meses en declive, sino que ha experimentado en los últimos tiempos su mayor debacle en lo que lleva de historia.

2. Naturaleza jurídica y relevancia penal-económica: Nuevos indicadores de riesgo derivados de la digitalización.

La cuestión referida a la naturaleza jurídica de estos elementos es, todavía, una cuestión discutida; podría decirse que aún no existe una doctrina unificada al respecto. Para empezar, en España «tanto los criptoactivos como los distintos actores implicados en su comercialización, se encuentran en principio fuera de regulación específica» (LEPERVANCHE,

2018, p. 10). Probablemente, debido a su gran variedad y a sus especialidades, no exista una solución única al respecto. El debate, al parecer, se deviene entre las siguientes posturas:

1ª) Criptoactivo como título valor impropio.

Se trataría de la postura más «clásica». De hecho, en la resolución vinculante V1029-15, de 30 de marzo de 2015, de la Dirección General de Tributos, la Agencia Tributaria se habría decantado por esta opción, dándole el trato de «anotación electrónica que incorpora el derecho a una cantidad de dinero; dado que no tiene el respaldo de ningún banco central, estaríamos ante un título valor impropio» (CHAMORRO DOMÍNGUEZ, 2019, p. 14).

La base de esta postura reside en la aserción de que los titulares de estos activos no incorporan ningún derecho ni existe un reconocimiento legal que así lo prevea. Mientras esto sea así, y continúen sin el amparo del banco central, el criptoactivo debería de tenerse como —de acuerdo con esta argumentación— un título valor impropio. En estos casos, el ejemplo que se aporta a modo de analogía es el de las tarjetas de crédito.

2ª) Criptoactivo como bien mueble digital.

En este sentido, se definiría el activo criptográfico como un «producto electrónico». Destaca en esta posición la argumentación de FERNÁNDEZ BURGUEÑO, que se aparta completamente de la idea de «moneda o activo financiero≫, igualando su naturaleza a la de, por ejemplo, una permuta. Básicamente, define los criptoactivos como «bienes muebles, digitales, no fungibles y de propiedad privada», amparando su razonamiento en los artículos 335, 337 y 345 del Código Civil español. Las notas características de los bienes muebles tradicionales podrían, según los defensores de esta posición, ser análogas a las de los criptoactivos y, por ende, ajustarse a una nueva concepción denominada como «bien mueble digital».

Continuando con la teoría que ofrece este punto de vista, su fundamentación radica en que los activos virtuales son «susceptibles de apropiación y pueden ser transportadas de un punto a otro» (CHAMORRO DOMÍNGUEZ, 2019, p. 16), además de lo ya delimitado por FERNÁNDEZ BURGUEÑO en su definición. Hay sectores de la doctrina que comparten el pensamiento de este abogado especializado en ciberseguridad y *blockchain* —entre otras materias—, incluso contamos con precedente jurisprudencial que consideraría los

criptoactivos —en realidad, más bien las criptomonedas, aunque extensible a este tipo de activos— como bienes muebles inmateriales: La STS 326/2019 los definía, de hecho, como «un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica» (Fundamento de Derecho TERCERO).

También se rechaza la idea de que puedan ser dinero de carácter electrónico. La Ley 21/2011, reguladora de la materia en cuestión, define el dinero electrónico como «todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor» (artículo 1.2); siguiendo la definición, no encajaría en el concepto. Este tipo de activos no tienen emisor, y aunque sí es cierto que tienen un valor fijado en un mercado, sigue sin ser dinero *fiat.*

Por toda esta serie de motivos, muchos se han inclinado a pensar que la categoría criptográfica de activos sería más encajable en esta naturaleza jurídica. Los hay como IBÁÑEZ JIMÉNEZ (2018, p. 118) que consideran que «los regímenes jurídicos nacionales deben, debido a la descentralización de estos activos y a la deslocalización de sus lugares de emisión, establecer mecanismos de coordinación para su calificación jurídica y consideración como activos no monetarios de naturaleza singular, asimilables a bienes mobiliarios o títulos de propiedad incorporales».

3ª) Criptoactivo como simple divisa o medio de pago.

Esta idea viene respaldada por cuestiones de uso o funcionalidad: «Las principales funciones de las divisas son actuar como medio de pago, servir como unidad de medida del valor de los precios de los bienes y servicios, y servir como instrumento de ahorro para ser recuperado en el futuro» (CHAMORRO DOMÍNGUEZ, 2019, p. 17).

La realidad es que los criptoactivos no poseen respaldo de ningún Banco Central, ni son reconocidas legalmente como divisa o medio de pago en ningún Estado, ni siquiera existe una obligatoriedad de uso; al contrario, tienen carácter voluntario. Así las cosas, el planteamiento encuentra amparo en lo dispuesto por una resolución del Tribunal de Justicia de la Unión Europea (fecha 22 de octubre de 2015, asunto C-264/14), en la que se entendía que las operaciones de *exchange* o cambio de moneda de curso legal por moneda digital expresan «prestaciones de servicios a título oneroso», cuya finalidad no es sino la de ser un medio de pago.

El TJUE tuvo que distinguir, para respaldar su argumentación, entre lo que serían las divisas tradicionales y las no tradicionales, siendo estas últimas «operaciones financieras, siempre que tales divisas hayan sido aceptadas por las partes de una transacción como medio de pago alternativo a los medios legales de pago y no tengan ninguna finalidad distinta de la de ser un medio de pago» (CHAMORRO DOMÍNGUEZ, 2019, p. 17). En definitiva, se hace en este sentido —y, al propio juicio—, un estudio algo confuso e intrincado de lo que se consideraría este criptoactivo: No lo admite como medio de pago de conformidad con la regulación aplicable, pero en el caso de que sea aceptada por las partes, entonces podrá ser considerado como medio de pago «análogo».

Si existe una certeza al respecto de la naturaleza jurídica de los criptoactivos, es que no hay regulación alguna que la concrete y, por ende, pareciera que su análisis va a depender en mayor medida de la rama del Derecho desde el que se observe.

Se representan así nuevos retos a través de los casos en los que medien criptoactivos para delinquir, y más específicamente para blanquear. Inmediatamente, surge la cuestión: ¿Cómo tratamos estos supuestos? Lo primero es conocer los nuevos indicadores de blanqueo de capitales, en concreto aquellos que puedan estar vinculados al uso de criptoactivos. Según MEGÍAS (2021), «los indicadores de riesgo de blanqueo de capitales se crean con la intención de mejorar las posibilidades de identificar actividades sospechosas de blanqueo de capitales, sobre todo con el uso de nuevas tecnologías como la criptomoneda».

El GAFI emitió un informe en marzo de 2021 a este respecto, para poder facilitar tanto al sector público como al privado la detección de actividades de dudoso carácter lícito, que puedan ser conductas de blanqueo. Algunos de los indicadores identificables en la materia podrían ser:

1. El carácter criptográfico de estos activos, dado que contribuyen a proteger la identidad del titular.
2. La opción de explotar otros países que no cuentan con sistemas de protección consistentes al respecto de los activos digitales como riesgo geográfico.
3. Estructuración de operaciones con activos virtuales en cantidades inferiores a los umbrales de alerta, proceder similar al tradicional.

4. Multiplicidad de transferencias inmediatas y, en general, la temporalidad y frecuencia en las operaciones con activos virtuales.
5. Patrones de operaciones dudosas o irregulares, en relación con el perfil del usuario, en especial si se trata de uno nuevo.
6. En definitiva, comportamientos que se consideran «inusuales» y que pueden indicar que se está cometiendo una actividad delictiva.

De este modo, se están ofreciendo datos que pueden resultar de suma utilidad a la hora de detectar y reportar estas conductas y facilitar, así, la supervisión y el cumplimiento de los pretendidos controles preventivos sobre el blanqueo de capitales y la financiación del terrorismo. A simple vista, no parecen indicadores muy distintos a los presentados en el sistema clásico de blanqueo, pero dadas las características singulares de los criptoactivos es muy importante atenderlas de forma independiente, separada. En cualquier caso, los indicadores de riesgo, para mayor utilidad, es conveniente que se vean reforzados con datos ofrecidos por institutos distintos al GAFI —por ejemplo, las autoridades policiales u otras fuentes de carácter público—.

En cuanto a la relevancia económico-penal que puedan tener los criptoactivos, lo cierto es que su no inclusión como moneda ni su consideración real como medio de pago nos coloca inevitablemente en una situación de «ausencia legal», vacío fácilmente aprovechable por los cibercriminales —adicionalmente a las propias características del sistema de codificación de la cadena de bloques— para sus fines delictivos.

El inicio de la preocupación por este fenómeno y, por ende, la relevancia cobrada empezó, en realidad, con el blanqueo de capitales cometido a través de criptoactivos y cuyo delito antecedente era el tráfico de drogas. En efecto, el crimen organizado ha protagonizado gran parte de la prensa reciente al respecto (por ejemplo, la operación Tulipán Blanca o el caso del portal *Silk Road,* entre otros casos). EUROPOL lanzó un informe en 2017 que revelaba que el blanqueo de capitales era uno de los principales motores del crimen organizado, siendo los criptoactivos —en especial el Bitcoin— los grandes protagonistas en esta actividad delictiva. No obstante, y dado que el método más habitual utilizado por las organizaciones criminales es la compra de criptomonedas, se analizará con mayor detalle en su apartado correspondiente.

3. Uso delictivo: Cuestiones preliminares.

Como avanzábamos en el epígrafe anterior, en el momento en el que el usuario o consumidor empieza a servirse de esta tecnología para delinquir a gran escala puede quedar justificada la intervención del Derecho Penal —pues conviene recordar que no cualquier conducta es merecedora de sanción penal—. A raíz de los indicadores de riesgo anteriormente expuestos pueden relatarse algunos supuestos de uso delictivo de criptoactivos.

Aunque no se trate del tipo penal sobre el que versa el tema, no es posible hablar de utilización fraudulenta de criptoactivos sin mencionar la gran estafa piramidal que han supuesto algunas inversiones en criptomonedas y que, de hecho, son casos que están siendo investigados actualmente por la Audiencia Nacional española. Así, *Arbistar, Nimbus,* o *Algorithms* lograron que sus inversores creyeran que iban a obtener una rentabilidad potente a raíz de sus inversiones en criptodivisas, pero lo cierto era que, sin saberlo, estaban llevando a cabo actos de disposición patrimonial en perjuicio propio. En este engaño se perfeccionaba la estafa, y difundiendo e impulsando esta creencia consiguieron seguir captando inversores, de modo que el fraude iba creciendo y con él el número de afectados.

Este tipo de comportamientos delictivos no acostumbran a ser aislados, sino que necesitan de otros actos también delictivos para evitar ser descubiertos, entrando en juego el blanqueo: Dado que se obtienen unos beneficios de forma fraudulenta, es frecuente la creación de sociedades ficticias en paraísos fiscales a las que llevar estas ganancias, no sin antes lograr una cadena de entramados y artimañas financieras para poder desplazar el dinero sin levantar sospechas. Y, como en cualquier supuesto de blanqueo, una vez se ha podido cubrir el rastro de los fondos, el dinero se incorpora al tráfico económico con apariencia legal.

En conclusión, partiremos de la base de que sí es posible blanquear dinero a través del uso de criptoactivos. El sistema es descentralizado, se utilizan técnicas muy concretas de cifrado, y la cadena de bloques no diferencia entre vendedores y compradores porque su «identidad» viene dada por códigos alfanuméricos. Es decir, anonimato garantizado.

De este modo, en los siguientes epígrafes se analizarán algunas de las nuevas formas que están usando los ciberdelincuentes para lavar dinero mediando criptoactivos.

III. MARCO OPERATIVO: ARTICULACIÓN DELICTIVA DEL CRIPTOACTIVO.

Se ha podido verificar que, en efecto, los criptoactivos poseen muchas cualidades de indudable carácter positivo que pueden ser utilizadas legítimamente, pero, como todo, tiene también una vertiente negativa: Su aprovechamiento para actividades delictivas y fines ilícitos, en especial para las conductas referidas al blanqueo de capitales. De hecho, en palabras del GAFI, «los activos virtuales […] tienen el potencial de estimular la innovación y la eficiencia financiera, pero sus características distintivas también crean nuevas oportunidades para que los […] criminales laven sus ganancias o financien sus actividades ilícitas» (2020, p. 2).

Ahora bien, también es cierto que, como declaró Josep Albors —Director de Investigación y Concienciación de ESET España—, «mucha gente puede pensar que utilizando criptomonedas […] no podrán ser rastreados. Sin embargo, esta es una idea errónea. Aunque es cierto que rastrear una cartera de criptomonedas o una transacción hasta una persona o una dirección IP no siempre es sencillo, tampoco es imposible» (BURRUECO, 2022). Esta última aseveración es fundamental de cara a estudiar no solo los siguientes apartados, sino el trabajo en su plenitud, ya que es de habitual resaltado el favorecimiento del anonimato en las transacciones con criptoactivos, pero únicamente por ser esta una de sus características más notables, no porque blinde la identidad del usuario en su totalidad. Consecuentemente, en todo momento hablaremos de obstáculos, pero nunca de imposibilidades.

En último extremo, se tratará en este capítulo de ofrecer una visión más específica de algunos supuestos conocidos de blanqueo de capitales con criptoactivos, a través de la investigación y exposición de los casos aparentemente más comunes en la práctica, según reportes, datos y noticias recientes.

A. La compra de criptomonedas.

El primero de los estudios es la compra fraudulenta de criptomonedas. En este tipo de supuestos será habitual presenciar cómo los delincuentes estafarán a sus inversores, para después tratar de lavar las ganancias que se hayan obtenido a través de este. Por ello, la mayoría de los ejemplos tratados van a verificar necesariamente un primer delito de estafa, pero conviene tener en cuenta que todos ellos originarán un posterior delito de blanqueo de capitales, pues solo así podrán utilizar unos beneficios que, realmente, son de origen «sucio» o ilícito. Esta es una de las dos razones por las que se incluye este método en un trabajo que versa sobre el blanqueo de capitales; la otra, reside en la frecuencia con la que se manifiesta esta táctica en la práctica.

Tal y como exponíamos, los delincuentes económicos estafan para después blanquear las ganancias. Se trata de las estafas de inversiones en criptoactivos, concretamente en criptomonedas. Si bien algunos de los artificios pueden adivinarse a simple vista, como por ejemplo una falsa promesa de obtener dinero gratuitamente, hay otros menos evidentes cuya técnica ha ido perfeccionándose con el tiempo. Actualmente, los criminales económicos suplantan identidades que, en un principio, pueden parecer medianamente fiables. Algunos aseguran pertenecer a grandes empresas, de reconocimiento internacional, lo que suele jugar a favor del ardid y, de hecho, es uno de los engaños que más víctimas genera.

Como muestra de esto, en febrero de este mismo año la Comisión Nacional del Mercado de Valores (en adelante, CNMV) alertó de que había detectado un fraude mediante el cual los delincuentes estaban suplantando su identidad vía telefónica. No olvidemos que la CNMV es un organismo entre cuyas funciones se encuentra la regulación de los activos en España. Al parecer, fue el epicentro de una campaña de *phising.* ¿En qué consistía el engaño, según relató la CNMV? Era simple: La víctima recibía una llamada desde un supuesto «departamento antifraude» —inexistente— del mencionado organismo, solicitando el interlocutor estafador datos e información personal. La táctica del fraude era presentar una oferta de compra de bitcoins que, aseveraban, habían sido incautados a una empresa que había sido falsamente acusada por la Justicia española. A raíz de ello, Fuerzas y Cuerpos de Seguridad del Estado y la presidencia de la propia CNMV empezaron a trabajar en un convenio que favoreciera la lucha contra el fraude financiero y protegiera, en el proceso, a los inversores.

Por su lado, el caso Arbistar, aunque —como indicábamos— se trata de una estafa, se llevó por delante a muchos inversores en criptomonedas que esperaban ver su inversión devuelta, sin que fueran realmente conscientes de que la intención inicial del administrador de la sociedad era quedarse con el objeto de dicho acto de disposición. Esta causa es uno de los procedimientos penales relativo a criptomonedas más sonados en la actualidad, siendo un gran ejemplo de lo que comúnmente se conoce como el esquema Ponzi. Se trata, en resumidas cuentas, de un ardid fraudulento de carácter financiero que, de hecho, recibe su nombre por la gran estafa llevada a cabo por el italiano Carlo Ponzi en el año 1900, y sigue un sistema muy similar al llevado a cabo por Santiago Fuentes —administrador de Arbistar—.

Como fuera, la Audiencia Nacional aceptó la instrucción del procedimiento, precisamente por el presunto carácter de macroestafa que revestían los hechos y porque territorialmente las víctimas pertenecían a distintas comunidades autónomas. Estamos ante el primer caso a gran escala de investigación penal por un delito cometido con criptoactivos —aunque se trate de una estafa—, lo cual resulta de suma relevancia de cara a futuros procedimientos que se inicien por causas análogas.

En el caso de Algorithms Group, se le imputaban a Javier Biosca —fundador— un total de nueve delitos, entre ellos: estafa continuada, apropiación indebida, blanqueo de capitales o delitos contra la Hacienda Pública, entre otros. Desde luego, la defraudación ascendía presuntamente a 818 millones de euros, y el número de víctimas se situaba en alrededor de los 3.000, según fuentes periodísticas, convirtiéndose en el fraude de mayor envergadura hasta la fecha en la temática que nos ocupa. El bróker utilizó la empresa para solicitar unas ciertas cantidades iniciales a los inversores que invertiría en diversas monedas virtuales. Prometía un beneficio de entre el 20 y el 25% semanalmente, que con el tiempo se iría reduciendo hasta, en un momento dado, no pagarles más: Aproximadamente un año después de empezar con la estafa, dejó de cumplir con los pagos a sus clientes y desapareció.

La operación «Tulipán Blanca», ya mencionada en epígrafes anteriores, es una de las más relevantes en cuanto a blanqueo con criptoactivos se refiere. Ocurrió en el año 2018, momento en el que fue desarticulada la banda que operaba entre España y Colombia, y que se dedicaba a blanquear el dinero que obtenían del narcotráfico por otras bandas también criminales, mediando el uso fraudulento de tarjetas de crédito y de criptoactivos. La investigación demostró que la organización procedía recogiendo en efectivo las ganancias ilícitas, para repartirlas en cantidades insignificantes y colocarlas en numerosísimas cuentas

bancarias —contándose 174 en total, y correspondiéndose este tipo de comportamientos con la técnica del *pitufeo*, explicada en el siguiente epígrafe—. Ya en Colombia, se retiraba el efectivo de sendas cuentas, pero este tipo de operaciones sí podían rastrearse sin mayor dificultad, motivo por el que las criptomonedas entraron en juego, y con ellas las autoridades finlandesas: Se determinó que el intercambio de los bitcoins se llevaba a cabo en Finlandia. Como ya se había adelantado previamente, la banda cayó en abril del 2018.

Por otro lado, se mencionaba también la operación *Silk Road* que llevó a cabo el FBI en 2013. *Silk Road* fue un portal que formaba parte de la *Deep Web*, y que sirvió de sede de comercio, fraude y blanqueo para los narcotraficantes. La juez Katherine Forrets condenó al fundador, Ross Ulbricht, a dos cadenas perpetuas, mostrándose severa a este respecto para marcar su posición con respecto al crimen organizado en la red; además, según narra POZZI (2015) en su artículo del diario electrónico «El País» al informar sobre los hechos, la imagen del Bitcoin quedó en su día muy perjudicada por este caso —es de sobra conocida la volatilidad de este activo virtual, una de las características que generalmente provoca la desconfianza en sus consumidores—.

B. El "pitufeo" como técnica de blanqueo.

El pitufeo es uno de los *modus operandi* más habituales para blanquear capitales. Explicado por la firma PricewaterhouseCoopers (en adelante, PwC), es «la división o reordenación de grandes sumas de dinero adquiridas por medios ilícitos, reduciéndolas a un monto mínimo que permite que las transacciones no sean registradas o, en su defecto, no resulten sospechosas. Dichas operaciones se realizan por un período limitado en distintas entidades financieras, o a través de pequeños giros dirigidos a una gran cantidad de personas que, generalmente, desconocen el origen de tales fondos» (PwC, 2015).

Debido a esta técnica, se obstaculiza en aún mayor grado que las autoridades puedan advertir el lavado de dinero: El delincuente repara con detalle en las cuantías que está blanqueando, de modo que no sobrepase los límites permitidos en la normativa que haya establecida al respecto.

Por otro lado, para MARK GAZIT (2019) —CEO de *ThetaRay*—, el pitufeo se puede entender de la siguiente manera: «Una transacción de US$0,25 nunca será detectada por un humano, pero con transacciones de este tipo pueden lavarse US$30 millones de dólares si se hace cientos de millones de veces». Así aparece relatado en el artículo de la BBC de BOWN (2019), que además explica un caso en el que miles de cajeros automáticos fueron programados para liberar billetes en un momento determinado de la madrugada, dinero que se recogía por las «mulas bancarias» —personas que a menudo son reclutadas para que lleven a cabo el blanqueo a través de sus propias cuentas bancarias, legítimas— y que después era cambiado a Bitcoin, usándose para financiar delitos como la trata de personas. Esto afectó, según relata la reportera, a entidades bancarias de al menos 40 países, y lograron en el proceso más de 1.000 millones de dólares.

En definitiva, la técnica del pitufeo aplicada a las criptomonedas supondría «cambiar a *cripto* cantidades relativamente pequeñas y repetidamente, durante meses. Bien pueden ser los propios criminales o personas contratadas por ellos con la promesa de recibir un porcentaje de la transacción» (G. GARCÍA, 2020). Correspondiéndose, con ese último grupo, las antes mencionadas «mulas»: Mensajeros que mueven de unas cuentas a otras el dinero ilícito; el vehículo del lavado de activos.

El papel de las mulas —no exactamente indispensable pero sí más atractivo para las organizaciones criminales, por cuanto no son ellos mismos quienes realizan la acción de mover el dinero— no siempre se lleva a cabo conscientemente. Hay que tener en cuenta que, en más ocasiones de las que conocemos, las personas que se convierten en «mulas» han sido sometidas a un engaño a través de una falsa oferta de trabajo. En España al menos este es un género de defraudación que el Código Penal también castiga —en su artículo 312— como un delito contra los derechos de los trabajadores, conducta subsumible en el tráfico ilegal de mano de obra, al reclutar trabajadores mediante engaño o falsedad en su oferta laboral.

Del mismo modo que las «mulas» del narcotráfico transportan droga, las «mulas de dinero» operan en sentido similar, pero cargando importantes sumas de dinero no declaradas. En todas sus modalidades las mulas son el eslabón más débil, el que más expone su seguridad y, en el caso del narcotráfico, su propia salud e integridad física. Su rol es fundamental porque ejecutan los movimientos fraudulentos para que los líderes de las organizaciones criminales no tengan que hacerlo: Por un lado, contribuye a disuadir a las autoridades, teniendo más

posibilidades de eludir su posible detención; por otro, y dándose el caso de que finalmente fuesen detenidos, su condena se podrá ver afectada por no ser la mano ejecutora del delito.
En el campo de la delincuencia económica, el *muling* no solo requiere transferir dinero de un país a otro, en ocasiones también se les fuerza a viajar para aperturar cuentas bancarias en el extranjero, que posteriormente van a servir para blanquear ganancias.

Las investigaciones del operativo «EMMA-7», llevado a cabo por las autoridades policiales en 2021, desvelaron que los perfiles de las «mulas de dinero» se dividían entre estudiantes, personas sin recursos económicos o, en menor medida, directores de empresas. En los dos primeros casos, la aceptación viene habitualmente vinculada a necesidades económicas: Los reclutadores conocen las formas de vender su argumentario, suavizando los riesgos a los que se exponen, y sus cebos no suelen ser verdaderamente conscientes de la naturaleza de los actos que perpetrarán. No obstante, la Policía Nacional continúa tratando de generalizar la advertencia de que existen ciertos sectores de la sociedad que, por su vulnerabilidad, serán el objetivo de las mafias para reclutarles como mulas de dinero. Poner punto final a este fenómeno pasaría por prevenir en primera instancia la captación de estas personas, un objetivo aparentemente inviable a efectos prácticos, pero que no admite rendición. Como fuera, el operativo se resolvió finalmente con más de un millar y medio de investigaciones penales abiertas y un total de 62 detenciones practicadas, en el marco de una acción global contra el lavado de dinero mediante la utilización de las mulas.

Retomando la casuística de esta modalidad, en un artículo del diario EL PAÍS, la periodista DELLE FEMMINE (2019) entrevistó a Alberto Redondo, comandante del grupo de delitos tecnológicos de la Guardia Civil, que explicó de forma muy llana la casi rutinaria actuación en estos supuestos por parte de los delincuentes económicos: «La forma general de actuar es la recepción de dinero en una cuenta bancaria dada de alta, en muchos casos con documentación falsa. También es usual la creación de la cuenta en bancos situados en terceros Estados […] En cuanto entra el dinero en la cuenta, es extraído rápidamente por las mulas […] Cada vez que interviene una mula, se queda con un porcentaje del dinero extraído».

Podría afirmarse que, en cuanto a investigación de estos delitos, el rol de las «mulas» cobra especial importancia, ya no tanto por lo que hacen sino las circunstancias que envuelven la propia acción. Esto es, sus cuentas, habitualmente sin apenas tráfico de dinero, de repente presentan entradas de cantidades considerables. Y, del mismo modo que se han recibido,

inmediatamente se retiran, lo que provoca que salten las alarmas. Así, una de las mejores bazas para que las autoridades puedan dar con las organizaciones criminales es poder identificar a estas «mulas», pues se representan como su mejor hilo conductor.

A modo ejemplificativo del método del *smurfing*, en el año 2019 cayó una red de blanqueadores que llegaron a lavar hasta 9 millones de euros en cuestión de tres meses, a través de cajeros de criptomonedas. Operaban en un locutorio de Ventas, Madrid, lugar en el que instalaron los susodichos. La Unidad Central Operativa de la Guardia Civil desarticuló la banda, que se dedicaba a lavar dinero procedente, entre otros, del tráfico de drogas, en la conocida como Operación Kampuzo. Según relata el diario español EL PAÍS al contar la noticia, los miembros de la OCU podrían haber intervenido otros instrumentos de custodia de criptomonedas —las llamadas «billeteras frías» y una veintena de *e-wallets*—. La realidad es que eran los mismos integrantes los que daban uso a estos cajeros de criptomonedas para mover, aunque a cuentagotas, cantidades ingentes de dinero hacia los monederos virtuales y llevarlas hasta Cúcuta, Colombia. Así pues, uniendo este apartado al anterior, la organización criminal simuló compraventas de criptomonedas emitiendo facturas de carácter fraudulento entre las empresas que figuraban en su propio entramado de sociedades pantalla.

Podría decirse que el establecimiento de cajeros de criptomonedas es el epicentro en el que predomina la técnica del pitufeo: El propio «criptocajero» emite un código QR —que ya viene asociado a otro código de 32 cifras y que equivale al valor asociado a la criptomoneda— y, así como este se obtiene, se pierde la pista del dinero.

En España existen, en la actualidad, más de 100 cajeros de *Bitcoin,* repartidos por todo el territorio, y se pueden encontrar en centros comerciales, en establecimientos destinados a dicho fin o incluso en negocios a pie de calle —desde tiendas informáticas hasta restaurantes—. Aunque existen cajeros que solo permiten la compra de criptomonedas, lo habitual será encontrar los que tengan habilitada tanto la compra como la venta de este tipo de activos digitales —lo que comúnmente se conoce ya como *exchange* de criptomonedas—.

Una de las ventajas que presenta la utilización de los criptocajeros es que se pueden llevar a cabo operaciones con dinero en efectivo, algo que Internet no permite —haciéndolo por esta vía se debe optar o por hacer transferencias, o bien por la utilización de tarjetas para poder realizar este tipo de movimientos—. Además, algunos de ellos no solo operan con Bitcoin, sino que también tienen habilitada la posibilidad de hacerlo con *ETH Ether, LTC Litecoin*, o *BCH Bitcoin Cash*, como ejemplos de criptomonedas más frecuentes.

C. El blanqueo en las casas de juego *online*.

Las casas de juego *online* son consideradas de los vehículos más potentes de traslado de dinero negro en todo el mundo. Las organizaciones criminales adquieren la licencia para montar su propia casa de apuestas *online* y utilizan testaferros para cubrir su rastro, pero realmente el lavado como tal empieza cuando las casas empiezan a estar operativas. ¿Cuáles son los mecanismos más habituales? Tal y como se describe en un artículo del diario EL PAÍS, «inyectar el dinero en la casa de juego *online* desde territorios donde no se controlan estos movimientos, contratar a personas que apuesten mediante tarjetas de crédito de prepago o poner a *bots* que aparenten jugar como si fueran usuarios anónimos» (G. GARCÍA, 2020). Todo el activo movido a raíz de lo apostado es ya de curso legal.

En la práctica, las casas de juego *online* se representan como la tapadera idónea paras las propias mafias, que van a ser los sujetos más habituales en esta modalidad concreta. Lo cierto es que los casinos brindan una gran facilidad para que las organizaciones criminales muevan las divisas, por no hablar de la utilización de criptomonedas para sus fines, aprovechando un sector que, en muchos países, no está prácticamente regulado.

No obstante, hasta la fecha se ha llevado a cabo en establecimientos físicos, y aunque la idea de crear casinos de criptomonedas esté en valoración, en la actualidad no es una praxis afianzada debido a esa inseguridad que los criptoactivos generan en los propios consumidores. Además, las autoridades permanecen vigilantes, lo que sumado a lo anterior podría mermar la intencionalidad del ciberdelincuente de optar por estas vías comisivas en concreto.

En el caso de España, desde que en 2012 se legalizara el juego *online*, el Ministerio de Consumo —y, en concreto, la Dirección General de Ordenación del Juego (en adelante, DGOJ)— ha ido implementando protocolos regulatorios severos con el fin de lograr un uso seguro y responsable de esta modalidad de juego, y únicamente van a poder adquirir licencias, en base a estos, los operadores que puedan garantizar los derechos de los consumidores (esto es, depósitos, protección de datos, las cantidades que se juegan y las cantidades que ganan, entre otros). Para tales fines, existe la Ley 13/2011, de 27 de mayo, de regulación del juego.

En la propia introducción de la nota técnica sobre la gestión del fraude de la DGOJ se incluye la prevención del blanqueo de capitales como imposición a quienes deseen adquirir la licencia para ofrecer actividades de juego de esta índole. Como una de las últimas novedades incorporadas, los sujetos obligados por esta Ley van a tener que elaborar manuales de gestión de riesgos a todos los efectos, detallando tanto los procedimientos como las medidas a implementar para identificar los distintos paradigmas delictivos que pueden darse durante su actividad y con qué medios cuentan para tratarlos.

Aunque este informe no incluya concretamente la utilización de criptoactivos para perpetrar los fraudes descritos, se espera que se empiecen a consagrar este tipo de nuevas necesidades en un futuro próximo, de cara a posteriores modificaciones legislativas, de modo que puedan subsumirse en los contextos de fraude que compone la nota técnica (fraude en los datos de identidad, en los medios de pago, en el origen de los fondos, relativo a la geolocalización o los amaños en apuestas deportivas). La intervención de los criptoactivos en estos supuestos deberá ser observada en próximas revisiones normativas, para lo cual se puedan establecer también controles de seguimiento y acciones preventivas.

Sí correspondería destacar, asimismo, la presumible intención de la DGOJ (2018, p. 16) de ir incluyendo estos supuestos, quizá de forma tácita, al incluir en el informe que «el sistema concreto de gestión de riesgos debe estar adaptado a la realidad de cada operador — tipos de juego ofertados, canales de comercialización usados, tipo de clientes, tipos de medios de pago admitidos o tecnología usada». Si bien no se hace mención específica al criptoactivo, puede dilucidarse de esta última aserción que estos podrían encajar, de cara a ser valorados por el sistema de gestión de riesgos al que los proveedores de estos servicios estarían obligados.

Prosiguiendo con la exposición de la problemática, muchos pueden llegar a preguntarse qué hace que las apuestas sean una vía tan conveniente para blanquear capitales: Como ejemplo ficticio, para ilustrar la respuesta a la anterior incógnita, se puede pensar en un individuo que ingresa la cantidad de 800€ de un *e-wallet* de criptomonedas en una casa de juego *online*. Este, que no llega a hacer ninguna apuesta excesivamente arriesgada, ingresa las ganancias que haya podido obtener en su cuenta bancaria. Dicho así parece sencillo, pero no debe obviarse que, como hemos señalado antes, los casinos están obligados al cumplimiento de la normativa antiblanqueo y están especialmente vigilados por las autoridades competentes, pero los delincuentes encuentran la forma de llevar a cabo

movimientos que no llaman la atención, que no sobrepasan los límites permitidos y que, en definitiva, no son susceptibles de hacer saltar las alarmas de los responsables de la supervisión y gestión de riesgos.

Asimismo, si se poseen los conocimientos y los medios necesarios para *hackear* perfiles de usuarios registrados, se puede mover con facilidad el activo de origen ilícito en las apuestas, suplantando su identidad. En España no está permitido para ninguna empresa con licencia, pero lo cierto es que este tipo de prácticas suponen, al menos, el 8% de las apuestas internacionales, y el método más frecuente lo constituye la utilización de las criptomonedas.

D. Coin Mixers: Tornado Cash.

La rúbrica de este apartado, en idioma anglosajón, da nombre a una suerte de mezclador *(mixer)* de criptomonedas, cuyo sistema está dirigido a ocultar directamente tanto el origen como el destino de una transferencia. También se les conoce por el nombre de «mezcladores de las redes oscuras» (NAVARRO CARDOSO, 2019, p. 22), teniendo como ejemplo paradigmático la moneda *Tor,* sobre lo que va a hablarse con mayor detalle en las próximas líneas.

El propio GAFI definía los mezcladores ya en el año 2014, como «un tipo de programa de anonimato que oscurece la cadena de transacciones en la cadena de bloques vinculando todas las transacciones a la misma dirección Bitcoin y enviándolas juntas de una manera que parezca que hubieran sido enviadas desde otra dirección». Los hay que equiparan su funcionamiento al de una coctelera —de ahí el nombre—: El *mixer* o mezclador, «a través de un proceso de mezcla, adquirirá las monedas y reenviará nuevos bitcoins aleatorios de otros usuarios que también realicen la operación de mezclado; sin que haya ninguna conexión entre los distintos participantes» (TENA PLATA, 2019, p. 26).

Este algoritmo se diseñó especialmente por la propia «comunidad cripto», con la finalidad de que los usuarios pudieran mezclar sus propias monedas con las de otros usuarios y así incrementar su privacidad, su anonimato. Se propicia así la innovación de herramientas que también protejan la identidad de sus usuarios. Este punto es máximamente beneficioso para quienes posean un gran número de criptomonedas, porque pueden ver reducidas sus

posibilidades de acabar siendo víctimas de extorsiones, *hackeos* o robos de sus criptodivisas. Otras de las ventajas son las ya citadas: el aumento de la dificultad de que sus fondos sean rastreados por las autoridades, así como del anonimato y la privacidad en las operaciones. Por último, y como aspecto más relevante en la materia, previene de que algunos criptoactivos puedan ser calificados como «contaminados», al proceder de un acto delictivo previo.

No obstante, esta tecnología no es blindada: En primer lugar, las distintas plataformas de mezcla de monedas utilizan patrones, por ende, si estos se llegan a descubrir, podrían analizarse y descifrar las operaciones realizadas. Este es uno de los puntos que más preocupación despierta en los participantes, debido al elevado riesgo que implica, ello sumado a la probabilidad de que, si el consumidor utiliza un servicio de dudable reputación o fiabilidad, podría acabar siendo fácilmente víctima de estafa y robo; al fin y al cabo, no podemos olvidar que se está realizando un depósito en la cuenta central del sistema, y perfectamente podría ocurrir que ese dinero no fuera devuelto a su depositario.

Si se trata de una plataforma «buena» desde la perspectiva de su funcionamiento, en ese caso se dificultaría en sumo grado la labor de investigación de las autoridades competentes, y es por esta misma razón por la que a los ciberdelincuentes les resulta tan atractiva esta herramienta. Tras el proceso mezclador, las criptodivisas derivadas de una actividad ilícita previa se dividirían y se representaría como un medio idóneo para blanquearlas. Chainalysis —firma especialista en inteligencia *blockchain*— ha emitido un informe recientemente que revela el aumento del uso delictivo de estas plataformas mezcladoras. Mientras que en 2021 se estimaba que solo un 12% de los fondos enviados provenían de actividades ilícitas, en el presente 2022 y sin que haya finalizado todavía ya se alcanza casi el doble del porcentaje —por ahora, un 23% de los fondos—. (Ver gráfico en ANEXO A).

A modo explicativo de esta tecnología, un usuario envía una cantidad de 5 bitcoins a una dirección determinada, a través del *mixer* elegido. Este último cobra una porción de esa misma cantidad a modo de tarifa por el servicio que está prestando y envía la parte sobrante a la dirección facilitada por el remitente, utilizando para ello diversas direcciones. Así es como se elude la vinculación remitente-destinatario, y así es como resulta tan sencillo ocultar la trazabilidad del cambio y blanquear las criptomonedas.

Los mezcladores pueden ser clasificados de la siguiente manera:

1. Mezcladores con custodia y mezcladores sin custodia.

De un lado, los mezcladores centralizados constituyen plataformas en las que los usuarios realizan el depósito y existe un ente controlador a través de un programa, que básicamente gestiona todo lo que entra: Mezcla las criptomonedas y las reenvía a los participantes. En este sentido, a mayor número de usuarios, más criptomonedas involucrarán el mezclado, y menos posibilidades de rastrearlas. Ahora bien, existe la posibilidad de que los propietarios de estos sitios web vendieran la información de los participantes, quedando al descubierto y, en el peor de los casos, siendo víctimas de estafas.

2. Mezcladores centralizados y mezcladores descentralizados.

De otro lado, los mezcladores descentralizados prometen una mucho más elevada garantía del anonimato. En este sentido, no existe un ente controlador, sino que los participantes se organizan por cuenta propia para poner a funcionar la coctelera de criptomonedas. En esta categoría de *mixers*, los usuarios operan con la certeza de que van a recibir la misma cantidad que depositan o no van a operar de ningún modo, así que se reduce considerablemente el ser víctima de robo de sus criptomonedas.

Existen muchos tipos de *Coin Mixers*, pero el que más revuelo ha causado ha sido *Tornado Cash*, hasta el punto de haber sido sancionada por Estados Unidos, sufriendo inmediatamente después un desplome del precio del *token* (aproximadamente un 56% de descenso del valor). Básicamente, *Tornado Cash* se trata de un «protocolo de *blockchain* para enviar y recibir transacciones anónimas mezclando tokens de Ethereum con un conjunto de otros tokens» (NELSON, 2022). El motivo por el que el Departamento del Tesoro de los Estados Unidos sancionó el sitio web fue porque aseguró que este estaba siendo usado por *Lazarus Group*, un grupo norcoreano de hackers, y que del mismo modo se había estado utilizando para blanquear más de 103 millones de dólares derivados del hackeo al puente *Horizon* de *Harmony Protocol* y a *Nomad Bridge*. Además, el caso no se ha quedado ahí: Muchos integrantes de la comunidad procedieron a su desconexión, y uno de los desarrolladores, Alexey Pertsev, fue detenido en los Países Bajos —al parecer, en Holanda habían iniciado a investigar criminalmente a *Tornado Cash* en el mes de junio del presente año—.

Conviene resaltar que el uso de los *Coin Mixers* no son ilegales, y que no todos los participantes intervienen con fines delictivos. Como en el mismo uso de la cadena de bloques y la tenencia de criptoactivos, no todos los usuarios son ciberdelincuentes, ni siquiera la gran mayoría. Es interés de muchos el poder realizar transacciones con privacidad y sin la implicación de intermediarios como los bancos, pero no por ello se está asumiendo que su intencionalidad es ilícita. Lo mismo ocurre con los servicios *mixers*, aunque interesa desde la perspectiva del desarrollo del trabajo el uso delictivo que se le ha podido dar a esta herramienta para delinquir. Como fuera, desde la costalada experimentada por *Tornado Cash,* este tipo de *softwares* vuelven a añadirse como una preocupación adicional para el consumidor.

Y, como no podía ser de otro modo, los hay que se han mostrado preocupados por la decisión del Departamento del Tesoro de Estados Unidos. *Electronic Frontier Foundation* (en adelante, EFF) es una organización sin ánimo de lucro cuya actividad se dirige, como ellos mismos declaran, a «defender libertades civiles en el mundo digital». A través de sus redes sociales esta entidad manifestó su preocupación por considerar que la sanción recaía sobre un proyecto informático de código abierto. Estados Unidos justifica dicha prohibición, por su parte, en la protección de la seguridad nacional, al revelar que el grupo ciberdelincuente norcoreano *Lazarus Group* intervenía como participante en la web para sus fines ilícitos.

Quizá parte del remedio resida, no en prohibir —pues normalmente los efectos de las prohibiciones no resultan ni preventivos ni beneficiosos, por más que se pretenda—, sino en hallar el modo de coexistir con estas plataformas y aprovechar sus utilidades, y regular allá se requiera control y supervisión para no minar los usos legítimos tratando de aplacar los fraudulentos. Esta suerte de conclusión podría, en realidad, aplicar a cualquiera de las modalidades comisivas que se han expuesto en este capítulo.

IV. MARCO JURÍDICO: ANÁLISIS DE LA NORMATIVA APLICABLE. CUESTIONES JURÍDICAS TRANSVERSALES. LA DIRECTIVA (UE) 2018/843.

En este capítulo procederemos a abordar el tema de estudio desde una perspectiva íntegramente jurídica. Para ello se va a llevar a cabo una localización general de la regulación nacional e internacional que existe al respecto; además, se evaluará la problemática que puede llegar a generar la escasez normativa, teniendo en cuenta que se trata de un fenómeno relativamente nuevo.

El motivo de dotar de un espacio concreto para el tratamiento de las vicisitudes legales que pueden producirse durante las distintas fases procedimentales no es sino la necesidad de aportar las propias conjeturas al debate jurídico: Teniendo en cuenta las dos variables mencionadas reiteradamente en el proyecto —el anonimato y la dificultad de trazabilidad de las operaciones—, ¿cuándo se entiende cometido el delito y cuál será el Tribunal competente para conocer de la instrucción o dictar sentencia? Cabe valorar, así, las distintas posturas doctrinales ofrecidas como medio compositivo para este tipo de cuestiones competenciales.

Se ha tenido en cuenta, además, como cuestión jurídico-penal de cada vez mayor relevancia, la incorporación del decomiso como medida accesoria, su operatividad en supuestos de blanqueo de capitales con criptoactivos y cómo se lleva a cabo por las autoridades. Como veremos, se trata de un elemento que no deja de crecer, que continúa expandiendo su ámbito de aplicación.

Por último, se analizará la última directiva lanzada por el Parlamento Europeo y el Consejo, dado que es la primera en la que empieza a atisbarse una creciente preocupación por los riesgos derivados del tráfico virtual de activos criptográficos.

A. Regulación existente.

No puede decirse que exista una legislación específica para la materia que nos ocupa. Se trata, en realidad, de una expansión del manto preventivo respecto al blanqueo de capitales y la financiación del terrorismo hacia la utilización fraudulenta de los criptoactivos. En otras palabras, la normativa que prima se refiere al delito en concreto —se trata de normativa antiblanqueo— y solo en los últimos años esta ha empezado a regular las operaciones con estos medios digitales, debido a su auge y los correspondientes riesgos que entraña. Por otra parte, y por lo que se refiere concretamente a las criptomonedas, no es noticia que la Unión Europea quiere lograr una normativa exclusiva y armonizada al respecto —para lo cual se está preparando el «reglamento MiCa», enfocado hacia la regulación del mercado y la tributación del criptoactivo—.

Este reglamento está pensado, en términos generales, para la protección del consumidor frente a los riesgos derivados de la inversión en criptoactivos. El espíritu de la propuesta vela por la estabilidad financiera internacional, una de las grandes preocupaciones del Consejo y del Parlamento Europeo a la hora de dar nacimiento a esta nueva herramienta legal. Vamos a analizar algunos de sus puntos clave de manera superficial, incidiendo con más profundidad únicamente en aquellos que tratan el blanqueo de capitales y los criptoactivos:

En primer lugar, los proveedores de servicios de criptoactivos, nuevos sujetos obligados —también en España, a raíz del Real Decreto-Ley 7/2021, y concretamente su artículo 2.1—, van a tener la obligación de proteger los monederos virtuales del consumidor, ostentando incluso una cierta responsabilidad en el caso de que los inversores pudieran perder sus criptoactivos. Además, se incluye en el marco regulatorio cualquier abuso de mercado —manipulación de este u operaciones llevadas a cabo con información privilegiada, entre otros—.

Segundo, se le otorga importancia a un aspecto relativo a la problemática de los criptoactivos que, si bien es de consideración esencial, a priori no suele acaparar demasiada atención. Se trata de la huella ambiental y climática; los criptoactivos conllevan un consumo energético elevado, pero no es una cuestión a la que, hasta la fecha, se le haya dado prioridad. Ahora, con el reglamento MiCa, los agentes que pertenecen a este mercado estarán obligados a declarar información sobre dicha huella, y la Autoridad Europea de Valores y Mercados

estará obligada a realizar normas técnicas que recojan las principales consecuencias negativas de esta tipología de activos con respecto al clima y el medio ambiente. De hecho, la Comisión Europea habrá de investigar el impacto medioambiental de los criptoactivos y presentar un informe, así como implantar normas de sostenibilidad.

Más enfocado al eje central del trabajo, la propuesta no ha querido pisarse los dedos repitiendo normativa existente, por lo que aquellas disposiciones que ya forman parte de la legislación antiblanqueo serán excluidas del texto del reglamento. Ahora bien, sí va a exigirse a la Autoridad Bancaria Europea que mantenga un registro público de aquellos proveedores que desprecien las normas omitiendo su cumplimiento. Además, si la empresa matriz de los proveedores se encuentra en algún territorio «no cooperador fiscal» o se considera de «alto riesgo» en cuanto a posible actividad blanqueadora, estos tendrán la obligación de aplicar controles reforzados, con intención preventiva.

En España, el Real Decreto-Ley 7/2021 incorporó novedades en materia de prevención de blanqueo de capitales, entre ellas la ampliación de los considerados «sujetos obligados» para poder incluir los servicios de cambio de moneda virtual y moneda de curso legal y a los proveedores de servicios de custodia de los *e-wallets* —o monederos electrónicos—. Además, según establece el artículo 2.1, existe desde entonces una obligación de inscripción o registro de estos proveedores. No obstante, se comentará más ampliamente en el último epígrafe del presente capítulo, en cuanto que incorpora el contenido de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo.

B. Problemática respecto a la escasez normativa.

El hecho de que nos encontremos ante un fenómeno relativamente novedoso implica, inevitablemente, que no exista excesiva regulación normativa al respecto, o para el caso jurisprudencia consolidada que nos asista en la manera más adecuada de tratar la cuestión. Existe debate doctrinal, por supuesto, pero cuando nos acercamos al momento de crear una acusación o defensa jurídica al respecto, o a un hipotético enjuiciamiento por el placer de buscar una solución a problemáticas de este calibre, y sin antecedentes existentes, ¿en qué podremos basarnos?

El «problema», en este caso, parece evidente.

Si bien es cierto que la Unión Europea se está preparando para empezar a regular unificada y transversalmente el mundo de los criptoactivos, la realidad es que hasta la fecha no contamos con precedente legal de ningún tipo; por ende, no hay mucha más alternativa que partir de cero. Empezar a albergar nuevas formas de comisión de delitos, subsumir nuevos tipos de bienes jurídicos necesitados de protección en los ya existentes, y otro tipo de técnicas jurídicas y legislativas que permitan extender el manto de protección a aquello que realmente requiera de amparo.

Mientras esto no suceda así, nuevas dimensiones irán cobrando espacio en nuestras vidas, en nuestro día a día, comportándose «anárquicamente», sin control. No se trata de «sobrelegislar», pues tampoco se pretende desvirtuar la intervención *ultima ratio* del Derecho Penal, ni truncar las expectativas de la innovación financiera, sino de regular lo que necesite ser regulado para confrontar la sintomatología de la inseguridad jurídica, de los verdaderos riesgos que el uso delictivo de los criptoactivos esgrime; de evitar, en fin, que su mal uso o uso fraudulento impacten de forma severa en el propio tejido económico, tanto a nivel nacional como internacional, y ataquen directamente a los derechos de los usuarios.

Es probable que la Unión Europea no ande del todo desencaminada a la hora de desear fijar, primero, un marco internacional para la regulación de los criptoactivos. Es del todo necesario que se presente una legislación armonizada, de modo que exista un marco común para todos los Estados Miembros, pues sin duda esto va a facilitar el tratamiento de los asuntos transfronterizos y podría además favorecer el mercado económico, entre otros beneficios.

De hecho, en ello se encuentra: El Comité de Asuntos Económicos y Monetarios del Parlamento Europeo ya avanzaba, este mismo año, hacia la gestación de un «marco legal uniforme» para este universo criptográfico. Todavía queda por delante un largo camino por recorrer, eso es indudable, pero empiezan a advertirse las preocupaciones que esta escasez normativa genera y esto es únicamente el comienzo. Que en la actualidad exista una escasez de normativa y —directa o indirectamente vinculado— de jurisprudencia, no implica que la cuestión permanezca estática. Al contrario, la Unión Europea busca conseguir una refundición del marco jurídico europeo, una tarea del todo ardua y más que ambiciosa.

De cualquier modo, la cuestión de la falta de regulación específica y las manifiestas intenciones de poner fin a este hecho no está exenta de problemática, ya que de un lado se

encuentran aquellos que abogan por una necesaria regulación de los criptoactivos y, frente a ellos, hallamos a quienes defienden la impenetrabilidad de la *blockchain*, tildando de intervencionista la acción reguladora en un ámbito que, *per se*, no nació para ser reglamentado. Por ende, la controversia «prorreguladora» *versus* «contraintervencionista» no promete resolverse pronto, aunque todo apunta a que la justificación de la necesidad de regulación encontrará el modo de imponerse sobre las excelsas y atractivas cualidades de la cadena de bloques, cuestión que, no cabe duda, acabará generando protestas y complicaciones, o bien, hará que el uso de esta tecnología se desplome hasta hacer perder el interés y la confianza de sus usuarios. Sin poner en duda, por supuesto, que reinventarán lo reinventado y hallarán nuevas formas de poner a prueba a la Criminología y al Derecho.

C. Vicisitudes procesales y penales: Cuestiones de competencia. El decomiso.

Como ya adelantábamos con anterioridad, una de las cuestiones que más controversia ha generado es la relativa a la determinación del juez competente en el seno del procedimiento penal, para la investigación de esta tipología de delitos. El sistema de la cadena de bloques asegura y protege la privacidad de las operaciones y los usuarios pueden encontrarse en distintos países; por ende, ¿cómo atribuir el lugar de comisión del delito y, consiguientemente, la competencia del asunto?

En este sentido, el fuero principal establecido por la Ley de Enjuiciamiento Criminal vigente en España —concretamente en su artículo 14.2 a 14.4— es, precisamente, la regla que no ofrecería respuestas para esta problemática: se trata del *forum commissi delicti*, que atribuye la competencia territorial al juzgado del lugar donde se ha cometido el hecho delictivo. Por eso, cuando se puede entender que dicho hecho se ha llevado a cabo en distintos lugares, aparecen otras reglas que se han generado a tal efecto y que podrían garantizar resoluciones factibles para subsanar la situación: La teoría del resultado, de la actividad o de la ubicuidad.

Por un lado, la teoría del resultado implica que se tendría en cuenta el lugar donde se produjo el resultado típico de la acción, en contraposición a la teoría de la actividad, cuyo

momento de la consumación se correspondería con el lugar en el que se ha realizado la conducta típica. De preferencia jurisprudencial, la teoría de la ubicuidad acepta tanto «el fuero del lugar de la realización de la acción como el de la producción del resultado»; no obstante, su aplicación está sujeta a condiciones: «siempre con criterio relativo, de indudable matiz casuístico», y «que conduzca a la solución más adecuada» (GENÉ CREUS, et al., 2013).

Según lo dispuesto en el acuerdo no jurisdiccional del 3 de febrero de 2005 sobre el principio de ubicuidad por la Sala Segunda del Tribunal Supremo, «el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa».

¿Cómo afecta esto a la materia que nos ocupa? Ante todo, es necesario partir de la base de que hablar de delitos en los que median aspectos tecnológicos inevitablemente implica el nacimiento de ciertas singularidades procesales. Ha sido reiteración expresa en este proyecto las consecuencias del sistema de *blockchain*, y ello porque se trata de tecnología punta que facilita la ocultación de los hechos delictivos, el encubrimiento de su rastro e incluso la eliminación de pruebas; la difuminación del parámetro espacio/tiempo, la garantía del anonimato del usuario… En este sentido, se obstaculiza en sumo grado la tarea de determinación de competencia y, precisamente, lo idóneo —y la razón por la que surgen las teorías previamente citadas— es reducir las cuestiones de competencia y evitar posibles demoras de cara a la instrucción y posterior enjuiciamiento. Además, la transnacionalidad sumada a la amalgama heterogénea y diferenciada de legislaciones a nivel internacional simplemente refuerzan el sentido y la existencia de este principio de la ubicuidad.

La problemática adquiere aún más fuerza en los países en los que, directamente, no existe una regulación al respecto. El coronel Juan Salom, destacado por haber liderado el Grupo de Delitos Telemáticos de la Guardia Civil, ya admitía en el año 2007 que el «Internet es algo muy rápido, que evoluciona día a día, y a veces la capacidad legislativa de los países no permite adaptar con celeridad sus leyes a las nuevas tecnologías». Las carencias legislativas cimientan los denominados «paraísos informáticos»: Lugares donde la normativa es laxa, circunstancia que aprovechan los delincuentes económico-informáticos para llevar a cabo su actividad delictiva.

Ahora bien, no en todos los casos se opta por la teoría de la ubicuidad. De hecho, en los últimos tiempos se ha tendido a desplazarla a favor del criterio de la eficacia en la instrucción,

que habilita la determinación de competencia dependiendo del lugar en el que «la investigación policial pueda tener algún éxito, donde se hayan realizado elementos del delito, donde puede operarse sobre los ordenadores informáticos y donde la instrucción puede ser eficaz» (Fundamento de Derecho Segundo, ATS 21 de octubre de 2015).

Del mismo modo, el Convenio de Budapest sobre el Cibercrimen de 2001 —ratificado por España en 2010—, en su artículo 22.5, determina que en estos casos la competencia corresponderá al Estado «que esté en mejores condiciones para ejercer la persecución del delito». Lo más acertado parecería acudir a las circunstancias de cada caso concreto, en especial al tratarse de supuestos en los que fácilmente pueden intervenir terceros Estados. Aún así, debemos servirnos, para dar resolución a este asunto, del acuerdo del pleno del TS antes citado (adoptado a fecha 3 de febrero de 2005): En materia de delitos de carácter informático, el criterio idóneo a seguir es el de la ubicuidad, ya que por sus características otorga competencia a los tribunales tanto del lugar en el que se lleva a cabo la acción, como al del lugar en el que se produce el resultado.

Por lo que se refiere al decomiso, el Código Penal esgrime en su artículo 127 bis: «el juez o tribunal ordenará también el decomiso de los bienes, efectos y ganancias pertenecientes a una persona condenada por alguno de los siguientes delitos, cuando resuelva, a partir de indicios objetivos fundados, que los bienes o efectos provienen de una actividad delictiva, y no se acredite su origen ilícito: […] i) Delitos de blanqueo de capitales». Así, el Código Penal habilita el decomiso en situaciones de blanqueo de capitales.

A nivel global, ya han trascendido algunos casos de incautación de criptoactivos. Por ejemplo, en Reino Unido se hizo la primera subasta pública de bitcoins que habían sido requisados anteriormente por las autoridades policiales británicas. Las criptomonedas volvieron a ser puestas en circulación, y se vendieron por un valor de 300.000 libras. En España, la Policía Nacional desarticuló en 2019 una banda criminal cuya actividad se movía entre las estafas y el blanqueo de capitales. Tuvieron que intervenir hasta 250.000 euros en bitcoins, que además se hallaban custodiados en diversas *wallets* y casas de cambio.

De manera similar ocurrió en 2018, la Guardia Civil desmanteló una organización criminal que distribuía sustancias psicoactivas a través de webs especializadas, usando como medio de pago el Bitcoin. Se requisaron ni más ni menos que 509 bitcoins, un total de 4,5 millones convertido a euros. Se trató, en aquellos momentos, de la mayor intervención en

Europa debido al valor incautado. También decomisaron 137.000€ en IOTA y 30.000€ en Stellar (XLM), otras criptomonedas quizá de menor reconocimiento, pero por cantidades también considerables.

Como último ejemplo, la operación Guatuzo llevada a cabo en 2018 por la Guardia Civil que se iniciaría a raíz de inteligencia ofrecida por la DIJIN de Colombia. Se probó que se había blanqueado aproximadamente 2.5 millones de euros, utilizando varias de las técnicas que se han estudiado previamente en este trabajo, como el *smurfing* o la compraventa de criptomonedas. Aún así, no se pudo desarticular la banda hasta la operación Kampuzo en 2019, acumulando un total de 9 millones de euros blanqueados a través de criptoactivos. Esta impresionante cantidad se dividió, al parecer, entre dos cajeros de criptomonedas, 4 billeteras frías y otros 20 *wallets*. Todo ello fue decomisado por las autoridades.

Ahora bien, ¿qué obstáculos puede encontrar el decomiso en estos casos? Por un lado, existe un órgano de la Administración que, si bien no es generalmente conocido, se encarga de dar soporte a los órganos judiciales a la hora de llevar a cabo actividades relacionadas con el decomiso, como la gestión de los instrumentos o bienes incautados. Se trata de la Oficina de Recuperación y Gestión de Activos (en adelante, ORGA). Pero lo cierto es que ni la ORGA ni las Fuerzas y Cuerpos de Seguridad del Estado parecen tener sólidos protocolos de actuación al respecto, dependen en todo momento de disponer de autorización judicial para decomisar y, de todos modos, no es fácil llevarlo a cabo a menos que puedan dar con el ciberdelincuente en situación de delito flagrante, o como mínimo con el monedero abierto (TENA PLATA, 2019, págs. 36-37), ya que estos requieren de clave y contraseña para poder acceder.

Por otro lado, una vez decomisados, ¿qué ocurre con con esos criptoactivos? El procedimiento que viene siguiéndose en España es el siguiente: «Una vez las criptomonedas se trasvasen a los *monederos policiales*, y, previa autorización judicial, serían intercambiadas a monedas de curso legal […] para posteriormente ser depositado (el valor de cambio) en la cuenta de consignaciones del Juzgado abierta para la causa penal concreta» (TENA PLATA, 2019, p. 37). Si finalmente el investigado fuera absuelto se procedería a la devolución de las criptomonedas, aunque habría que tener en cuenta, y esto es muy importante, que estas ya han sido anteriormente intercambiadas por monedas de curso legal, pudiendo haberse producido en el proceso alteraciones en su valor.

Las opciones, pues, del investigado absuelto se limitan a la solicitud de devolución de sus criptomonedas, con posibilidad de exigir responsabilidad patrimonial frente a la Administración de Justicia (Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público).

Señalar, por último, la importancia que se le da al decomiso en la legislación penal vigente en nuestro país, para mayor compresión de porqué dedicarle un área en este apartado. Se trata, en primer lugar, de contribuir a ese gran fin ya mencionado con anterioridad de que la comisión de un delito no resulte provechosa para nadie. Así pues, el decomiso de los ingresos que genera la actividad delictiva se ha venido considerando un método eficaz para combatir la criminalidad organizada. Los casos aquí expuestos dotan de una visión aproximada a la importancia del decomiso, dados los desorbitados valores que han conseguido incautarse y que, de no haberlo hecho, todavía estarían en posesión de los blanqueadores.

Parece un enfoque acertado orientar la finalidad del comiso a privar al delincuente criminal del motivo por el que generalmente delinquen: las ganancias. Por lo cual, es perfectamente comprensible que se trate, en la actualidad, de una de las más «poderosas» estrategias de la Unión Europea para luchar contra los delitos económicos y, en concreto, contra el blanqueo de capitales.

Ahora bien, como todo, la Comisión Europea parecía estar planteándose la posibilidad de continuar ampliando los supuestos de decomiso, según detalla AGUADO CORREA (2013) en uno de sus artículos referido al decomiso. Aunque estos planteasen las garantías necesarias, podría volver a ser objeto de crítica por parte de ese sector doctrinal que, de primera mano, ya consideraba la tipificación autónoma y extensiva del delito de blanqueo de capitales como una respuesta innecesaria al discurso del riesgo. Esto es, como el camino a la desvirtuación del principio de intervención mínima del Derecho Penal y como una consecuencia de su modernización, hasta el punto de penar en base a indicios o que se deje de considerar necesaria la existencia de una condena previa, tal y como se ha concluido en apartados anteriores.

En este sentido podría resultar más favorecedor mostrarse más parco con la incautación de estas ganancias, y reforzar la acción requisitoria. Es decir, hacer ver al delincuente económico que sus acciones delictivas no van a ser impunes y que, además, estas van a ser en

vano porque no va a poder aprovechar los beneficios que estas le pudieran haber reportado. La cuestión negativa es que en la práctica no parece estar dándose tanto como debiera, de modo que sería conveniente reorientar las políticas existentes a una reforzada aplicación de la cultura del decomiso, y a blindar sus métodos si es necesario, pues solo de esta manera esta herramienta preventiva tendría mayor calado en los criminales.

D. Novedades legislativas: La Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo.

Esta directiva, conocida comúnmente como la «V Directiva», es el primer intento de delimitación del blanqueo digital. Hasta ahora, esta serie de directivas dirigidas a la lucha contra el blanqueo de capitales y la financiación del terrorismo no habían albergado ni a los proveedores de servicios de moneda electrónica, ni a los servicios de cambio de moneda virtual y de curso legal; tampoco se había llegado a hablar de salvaguardas de monederos electrónicos, lo que de algún modo refuerza la razón de ser de este estudio. La necesidad de controlar estos nuevos operadores vino inspirada por los últimos diagnósticos del GAFI, con quien la Unión Europea ha acostumbrado a mostrarse en consonancia y con un profundo respeto por la información que recaba y facilita en su incesante lucha contra los delitos de blanqueo de capitales y financiación del terrorismo. Todo lo relativo a estas figuras se encuentra entre las modificaciones más novedosas que se han llevado a cabo en la V Directiva (2018/843), y que dan una importantísima pista de la dirección que está tomando la preocupación por esta problemática.

¿De qué forma se integran en la normativa estos conceptos? Bien, la idea principal es que existe un listado de sujetos que quedan obligados al cumplimiento del contenido de la directiva. Si bien ya estaban delimitados en un principio, con la modificación se adhieren algunos más a dicha relación de operadores, adaptándose así a esas nuevas realidades que han ido plasmándose a lo largo del trabajo. Se trata de los proveedores de servicios de cambio de moneda virtual a moneda de curso legal, y también de custodia de monederos electrónicos. Los apartados (8) a (10) tratan de forma más o menos específica este asunto. Vamos a tratar de darle una definición aproximativa a estos términos:

1º) Moneda virtual.

La Directiva (UE) 2018/843 enmarca 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».

En un primer lugar, con esta conceptualización se está tratando de dejar claro que las monedas virtuales no son, independientemente del término, monedas reales; en otras palabras, no sustituyen a la moneda de curso legal. Es más adecuado, quizá, referirse a ello como criptoactivo o, más concretamente en el caso del dinero, como criptomoneda.

Si bien es cierto que generalmente los Estados no habían aceptado la moneda virtual como moneda de curso legal, en 2016 se empezó a hablar de que el gobierno japonés había mostrado una cierta predisposición a admitir el Bitcoin —y otras criptomonedas— como divisa. No hace mucho, en junio de 2022, el Parlamento de Japón finalmente impulsó una ley dirigida a la regulación de las monedas estables o *stablecoins*, que entrará en vigor en cuestión de un año desde su aprobación. La clave se encuentra en la vinculación de este dinero digital al *yen* japonés o a cualquier otra moneda de curso legal; en cualquier caso, se requiere la protección del derecho de los consumidores a cambiarlas por el valor nominal correspondiente.

2º) Proveedores de servicios de cambio de moneda virtual a moneda de curso legal y de custodia de monederos electrónicos.

Siguiendo la línea de la directiva, el primer tipo de servicios se define como «la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido». Se entiende que existen personas físicas o entidades dirigidas a permutar las monedas digitales por otras diferentes, de curso legal (*exchangers*). Es decir, intercambiar el criptoactivo o criptomoneda por su valor en una divisa concreta.

Por otro lado, los segundos operadores mencionados serán «aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas

virtuales». En este caso, lo que ofrecen los proveedores es albergar, en un espacio virtual, los activos digitales que poseen los consumidores. Es lo que se conoce como *e-wallet.*

En cualquiera de los casos, son sujetos que estarán obligados por un lado a cumplir con la nueva normativa y, por otro, a inscribirse en el registro correspondiente del Banco de España. Para tal efecto se ha habilitado el trámite propio a través de la Sede Electrónica del Banco de España, y deberá realizarse siempre y cuando sendos servicios se desarrollen en territorio español.

En España, el Consejo de ministros aprobó en abril de 2021 el Real Decreto-Ley 7/2021 por el cual se lograba finalmente la trasposición de la V Directiva (2018/843) a nuestro ordenamiento jurídico, y cuya publicación en el BOE consta el día 28 de abril.

Una de las incógnitas que había surgido a raíz del nacimiento de esta nueva imposición es si quebraría el anonimato de las transacciones al llevarse un registro público de estos proveedores de servicios. La respuesta que se ofrece a este planteamiento es negativa, pues la privacidad de la identidad sigue manteniéndose en prácticamente todo el entorno del activo virtual: Los usuarios pueden seguir llevando a cabo sus operaciones al margen de sendos operadores.

El fundamento de esta nueva imposición reside en la posibilidad de que el SEPBLAC —y, en términos generales, todas las unidades de inteligencia financieras— pueda obtener la información necesaria para asociar la dirección de un criptoactivo a su propietario, pues es la manera de poder investigar si se está usando o no fraudulentamente. De no poder acceder a este tipo de información, las investigaciones se convertirían prácticamente en labor imposible. Lo cierto es que la Unión Europea ya viene manifestando sus intenciones de tener identificados a quienes poseen criptoactivos, si empieza a generalizarse su uso.

Lo cierto es que, en realidad, la razón de ser de la modificación de la Directiva anterior vino de mano del Plan de Acción de la Comisión Europea contra la financiación del terrorismo, a causa de los en su día recientes atentados terroristas que se cometieron en territorio francés en noviembre de 2015. Independientemente de que se ha resaltado continuamente la importancia de las novedades legislativas en materia de blanqueo y criptomonedas, la V Directiva alberga muchos más cambios, aunque ha de reconocerse que la inclusión de estos nuevos operadores jurídicos como sujetos obligados era una de las modificaciones más esperadas.

Con su sujeción a la normativa antiblanqueo se espera de ellos que reporten movimientos que puedan tildarse de sospechosos por suponer conductas fraudulentas (de blanqueo de capitales, de estafa, de financiación del terrorismo…), aspecto que ha generado altas expectativas preventivas que, por ahora, desconocemos si darán el resultado esperado. También parece que la V Directiva apremia, de algún modo, a que estos proveedores de servicios de custodia o intercambio «restrinjan parcialmente» el anonimato de las criptomonedas.

Esta última parte puede llegar a ser la cuestión más controvertida de todas, en tanto que estaría afectando a una de las premisas fundamentales de los criptoactivos y, sin la cual, estos perderían todo su atractivo y utilidad, volviendo a incurrir en una frustración de las expectativas de innovación financiera de los usuarios. Así, se trata de una cuestión considerablemente delicada, ya que difícilmente se va a poder ejercer algún tipo de control sobre los activos criptográficos sin golpear en seco las especialidades que, en primer lugar, le otorgan su razón de ser. Más que probable, se puede afirmar con certeza que esta va a ser una cuestión que todavía va a generar aún más polémica, en cuanto se produzcan más avances legislativos —y, para algunos, más recortes en su libertad de posesión y uso de criptoactivos—
.

Por último, resaltar al antes mencionado SEPBLAC, como autoridad supervisora en prevención de blanqueo de capitales que es, conformándose como la unidad de inteligencia financiera vinculada al Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España. Opera como órgano de apoyo de la Comisión de Prevención del Blanqueo de Capitales, y es la entidad a la que se deben reportar indicios o pruebas de que se están cometiendo hechos delictivos orientados al blanqueo de capitales o a la financiación del terrorismo. De no hacerlo, los individuos pueden estar sujetos a sanción además de a responsabilidad penal, con lo cual, existe una verdadera e importantísima obligación de informar a las autoridades, al constituirse como una de las herramientas preventivas más eficaces.

Las funciones del SEPBLAC más relevantes en materia de blanqueo de capitales son:

1. Reforzar la colaboración y apoyo a autoridades durante las investigaciones de este tipo de delitos —y otros, de consideración también grave—.
2. Colaborar también con las UIFs de otros Estados.

3. Lidiar a nivel global con los riesgos más graves originados por las conductas de blanqueo de capitales, tratando de promover una actuación unitaria y coordinada en aras de prevenir y consolidar las investigaciones y regulaciones.
4. Ejercer de órgano de soporte a autoridades judiciales y policiales.
5. Recibir las correspondientes informaciones, antes citadas, al respecto de hechos o indicios de comisiones delictivas relacionadas con blanqueo de capitales. Analizar lo obtenido y consignar el procedimiento más adecuado en cada caso concreto, de corresponder.
6. Supervisar y controlar que las imposiciones a los sujetos obligados por la normativa antiblanqueo se están cumpliendo por parte de estos.

Estas son únicamente algunas de las funciones que desarrolla el SEPBLAC, habiéndose mencionado las que más inciden en la lucha contra el blanqueo de capitales, pero son suficientes para revelar la importancia del papel que desarrolla este instituto en nuestro país.

V. CONCLUSIONES.

A raíz de la digitalización, hemos asistido a una inevitable modernización de los métodos empleados por los criminales para llevar a cabo su actividad delictiva, siendo uno de los más ilustrativos ejemplos el uso fraudulento de tecnología punta para blanquear dinero. La mera posesión de criptoactivos no es ilegítima; sí lo es, por contra, utilizarlos para convertir las ganancias derivadas de la comisión de un ilícito en dinero de curso legal, siguiendo en el proceso el mismo esquema descrito por el artículo 301 del Código Penal. Es lo que se ha tratado, en esencia, de analizar a lo largo del trabajo: La injerencia de las nuevas tecnologías en los delitos tradicionales y qué métodos se han avistado más frecuentemente en la práctica, sin obviar la evidente preocupación que estos están despertando y cómo afectan a la lucha global contra el blanqueo de capitales.

A la postre, se han podido extraer las siguientes conclusiones:

PRIMERA.- Que, por la propia naturaleza de la cadena de bloques *(blockchain)*, los criptoactivos reúnen una serie de características de alto atractivo para el perfil del ciberdelincuente: codificación, alto nivel de privacidad y anonimato, dificultad de trazabilidad de las operaciones, no intervención de intermediarios y descentralización. El tratamiento del blanqueo de capitales tradicional ya era, *per se*, complejo y controvertido; ahora, con estas formas avanzadas, se presentan nuevos retos para el Derecho: No tanto en la afección al tipo penal, que mantiene su operatividad, sino en la forma en la que estos atributos contribuyen a facilitar notoriamente el lavado de dinero, además de los obstáculos que se interponen para su efectiva investigación.

En este sentido consideramos que, ante esta nueva realidad, el Derecho no tiene más remedio que adaptarse —algo que, por otro lado, siempre ha hecho de una forma u otra—. Los criptoactivos, por su lógica interna, no parecen ser susceptibles de sujeción a ningún ordenamiento jurídico, porque por sus características inherentes difícilmente se podría regir por otro sistema que no sea el suyo propio: Tienen sus propias normas y este es gran parte del «encanto» que mueve a tantos inversores.

Aún así, continúan sucediendo avances que vuelven a quebrar los esquemas previos: Como se ha señalado con anterioridad, Japón decidió dotar de carácter legal a una criptomoneda: el Yen Digital, que cuenta con respaldo institucional. La cuestión aquí relevante es que, con esta regulación, ya se ha perdido una de las características notables de la criptografía: La descentralización. El Banco Central de Japón controla su funcionamiento, y el Yen Digital está respaldado por el yen físico, de modo que no lo sustituye sino que es meramente complementario. Esta cuestión entronca directamente con la tratada en la conclusión segunda.

Con todo, queda verificado que el avance de las nuevas tecnologías nos ha llevado a presenciar constantes reinvenciones por parte de los ciberdelincuentes, quienes han llegado a dar con nuevas y elaboradas maneras de continuar delinquiendo, saliéndose de los esquemas tradicionales, quizá ya trillados en exceso. A la cuestión de si los criptoactivos pueden ser utilizados con fines delictivos la respuesta es inequívocamente positiva, ello independientemente de los que sí los usen con fines legítimos.

SEGUNDA.- Que, a causa de la escasez regulatoria en la materia y la creciente preocupación que está generando, el legislativo —a nivel internacional y, por extensión, a nivel nacional— oscila entre pecar de intervencionista o velar por la protección de la libre economía, sin haber logrado hallar un punto intermedio. El mismo sistema que envuelve a los criptoactivos está ideado para evitar, entre otras cosas, que los Estados o las entidades bancarias y financieras intervengan en las transacciones; con todo, la preocupación que genera el uso fraudulento de estas posibilidades digitales coloca en el punto de mira los intentos regulatorios y si estos, de alguna forma, terminarán por viciar la innovación financiera. Muestra de ello la encontramos en el supuesto antes propuesto, el caso de Japón al regular el Yen Digital.

Hay otros países que también se encuentran trabajando en ello: En Estados Unidos, por ejemplo, se estaba planteando la intervención de las agencias federales para regularlos. El presidente Biden habría presentado una propuesta de marco legal para «el desarrollo responsable de activos digitales», admitiendo sus usos beneficiosos para el propio sistema financiero, pero supeditándolos a los riesgos que conllevan.

Lo más probable, a nuestro juicio, es que los riesgos acaben sobreponiéndose a la mencionada innovación financiera y se acabe viciando la esencia de la *blockchain*. Muchos

abogan por la imposibilidad de que esto ocurra, ya que la «magia» de la codificación y la descentralización es, precisamente, la inviabilidad de cualquier forma de intervención: No existe autoridad de ningún tipo en la *blockchain*, afirman. No obstante, se pueden hallar las formas de someter a regulación a los poseedores de criptoactivos, tal y como está empezando a hacerse en la práctica. Esto es, no se trata de regular el propio sistema de funcionamiento de la *blockchain* o, como caso extremo, incluso de la *Deep Web,* sino de legislar sobre los participantes, sobre los inversores, de modo que se tenga un control de las personas o empresas que están haciendo uso de los criptoactivos, así como de los operadores que se constituyen como proveedores de servicios de este tipo.

Por ello, se habla en este sentido de «difuminación» de la línea entre el «libre desarrollo» de la cadena de bloques y los propios límites de mercado.

TERCERA.- Que las dificultades de determinación del tribunal competente ocasionadas por la transnacionalidad intrínseca de la propia criptomoneda pueden superarse gracias a la solución aportada en el acuerdo del Pleno no jurisdiccional del Tribunal Supremo —ya citado—, en el que se configura la teoría de la ubicuidad como criterio idóneo a seguir. Debido a este postulado doctrinal, se va a poder entender cometido el delito en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, y de igual modo, en cualquier lugar en el que se hayan producido, del todo o en parte, los efectos de su comisión. Así, y en cuanto a la instrucción de la causa, podría ser competente el juez que hubiere iniciado en primer lugar las actuaciones procesales, sin que influya que los medios empleados para delinquir se puedan encontrar en un tercer Estado.

Explicado así, no parece complicado concluir porqué este criterio rompe las barreras competenciales y evita, al mismo tiempo, que se produzcan cuestiones de competencia que dilaten los procesos y sus correspondientes instrucciones. Se resuelve, entonces, a una de las vicisitudes de carácter procesal que más debate había generado, llegando a alcanzar un consenso para la efectividad de las investigaciones y el curso del proceso penal.

CUARTA.- Que, en efecto, y tras una búsqueda exhaustiva de noticias de prensa e informes institucionales recientes, se ha llegado a la conclusión de que las técnicas de recurso frecuente por parte de los cibercriminales son la compraventa de criptomonedas, el *smurfing*

a través de cajeros automáticos de bitcoins o el recurso a herramientas nuevas diseñadas a tal efecto, como las cocteleras de criptomonedas (comúnmente conocidas como mezcladores o *coin mixers).*

Estas nuevas formas pueden, *prima facie*, ser más relevantes desde una perspectiva criminológica que desde el punto de vista del Derecho Penal. ¿Por qué? La Criminología es una ciencia destinada al análisis de los crímenes que, por un lado, permitirá identificar el delito y, por otro, concretará las formas de prevenirlo. En cambio, a efectos penales, que para blanquear capitales se utilice como medio un criptoactivo no varía la penalidad ni la conducta, más cuando el propio tipo penal, conforme a su redacción actual, da cabida a modalidades comisivas tanto tradicionales como disruptivas, nuevas o futuras.

No obstante, y a modo conclusivo, no se puede tampoco obviar la manera en que estas nuevas formas inciden en el Derecho Penal Económico, por no mencionar las problemáticas a nivel regulatorio que empiezan a surgir y que, ahí sí, el plano jurídico debe entrar de lleno.

Inspira para la confección de esta conclusión la visión de VERA RIVERA (2017, pp. 52-53), al explicar que «si bien es cierto que la fundamentación jurídico penal y la criminológica no tienen relación […], se puede señalar que quien se ocupa del Derecho penal, tiene que conocer junto a las normas jurídico-penales y su interpretación, además, la criminalidad y el delito».

QUINTA.- Que la última modificación de la normativa internacional antiblanqueo empieza a cercar estas nuevas formas de lavar dinero, pasando por incluir operadores de servicios de custodia de criptoactivos y de intercambio de los mismos como sujetos obligados al cumplimiento de las medidas de prevención, sometiéndose a supervisión de las autoridades. Esto deja ver que la preocupación por el uso delictivo de los criptoactivos está creciendo globalmente y ello conlleva inexorablemente a la gestación legislativa como remedio paliativo del riesgo inherente, así como al planteamiento de propuestas preventivas que, por el momento, no revelan resultados concretos.

Y, a este respecto, lo que se debe pretender con sendas propuestas es, de hecho, convertirlas en herramientas útiles para la prevención de la «criptodelincuencia» sin que ello destroce las expectativas de innovación financiera de los consumidores. Se trata de una misión de indudable dificultad, ya que nunca resulta sencillo encontrar un término medio que contente y satisfaga a ambos extremos.

SEXTA.- Podría ser cuantiosamente valioso a efectos de encontrar fórmulas preventivas efectivas:

1. La colaboración por parte de los proveedores de servicios en la aportación de información que le pueda ser requerida, más allá de su registro como operador a tal efecto. Informar al SEPBLAC, en este sentido, de si se detecta algún tipo de uso ilegítimo de los criptoactivos que se cambien o se custodien. Esto es algo que ha empezado a preverse a raíz de la V Directiva.
2. Incidir en la supervisión, control y vigilancia en el caso de las empresas que posean u operen con criptoactivos. En este sentido, contar con un modelo de *Compliance* se puede representar como una gran opción para prevenir la comisión de delitos de manera interna, sin que requiera de acción legislativa.
3. Crear incentivos para personas físicas y jurídicas que reporten actividad sospechosa de constituir blanqueo de capitales a través de criptoactivos.
4. Generar protocolos de control y procedimiento sólidos y unitarios para una mayor efectividad de la actuación de las autoridades, así como dotar a los órganos destinados a la lucha contra el blanqueo de más facultades de investigación, control y supervisión.

A modo de desenlace, resaltar el papel decisivo que juega la prevención en nuestra sociedad para minimizar riesgos y, con ello, reducir los índices de criminalidad. El espíritu que se persigue manifestar con la composición de las legislaciones contemporáneas no pretende ser coercitivo; no está orientado a ser punitivo sino a ser preventivo. Promovemos, pues, el impulso de políticas más preventivas, y no tan persecutorias: Siempre habrá de primar, a nuestro juicio, la posibilidad de disuadir al perpetrador desde el inicio, sin obviar que, si esto resulta insuficiente, no podrá tampoco quedar impune su intento de enriquecimiento ilícito.

REFERENCIAS BIBLIOGRÁFICAS.

BIBLIOGRAFÍA BÁSICA.

- AGUADO CORREA, T. *Decomiso de los productos de la delincuencia organizada: "Garantizar que el delito no resulte provechoso".* Revista Electrónica de Ciencia Penal y Criminología, 2013. 27 p.
- CALDERÓN TELLO, L. F. *El delito de blanqueo de capitales: problemas en torno a la imprudencia y la receptación.* Madrid, 2017. 610 p.
- CHAMORRO DOMÍNGUEZ, Mª, C. *Aspectos jurídicos de las criptomonedas. Blockchain intelligence.* Madrid, 2019.
- DE MIGUEL ASENSIO, P. A. *Propuesta de Reglamento sobre los mercados de criptoactivos en la Unión Europea.* La ley Unión Europea, 2020, págs. 1-7.
- FERNÁNDEZ BERMEJO, D. *En torno al concepto de blanqueo de capitales. Evolución normativa y análisis del fenómeno desde el Derecho penal,* 2016.
- GARCÍA BERNÁRDEZ, M. *Blockchain y la Tokenización de Inmuebles,* Inmueble: Revista del sector inmobiliario, nº 177, 2017. págs. 60-63.
- GENÉ CREUS, J; BARRIENTOS PACHO, J. Mª; MELERO MERINO, J. *Prontuario Procesal Penal*. Ediciones Experiencia, 2013.
- GÓMEZ BENÍTEZ, J. M. *El delito previo al delito de blanqueo de capitales a vueltas con el delito fiscal.* Análisis GA&P, 2014, págs.. 1-3.
- IBÁÑEZ JIMÉNEZ, J. W. *Blockchain: Primeras cuestiones en el ordenamiento español.* Alasatria. Dykinson, 1ª Edición. 2018, 194 págs.
- LANDROVE DÍAZ, G. *El Nuevo Derecho Penal.* Tirant lo Blanch, 2010. 195 págs.
- LEPERVANCHE, L. *Consideraciones jurídicas sobre criptoactivos y petros.* Revista Venezolana de Derecho Mercantil, nº 1. 2018, 43 págs.
- MARTÍNEZ, F. R. *Prontuario jurisprudencial del delito de blanqueo de capitales.* Dykinson, 2020.

- MOUGAYAR, W. *The business blockchain: promise, practice, and application of the next Internet technology.* John Wiley & Sons Limited, *2016,* 179 págs.
- MUÑOZ CUESTA, F. J. *El delito de blanqueo de capitales. Alcance después de la reforma del art. 301 por LO 5/2010: autoblanqueo y delito discal. Revista Aranzadi Doctrinal, núm. 2, 2013, págs. 11-19.*
- PÉREZ MEDINA, D. *Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo*. Boletín Criminológico, 2020, 27 págs.
- ROMERO FLORES, B. Delito de blanqueo de capitales en el Código Penal de 1995. *Anales de Derecho.* Universidad de Murcia. Número 20, 2002, págs. 297-333.
- SAGRADO, O. M. *La determinación del bien jurídico protegido por el delito de blanqueo de capitales y el autoblanqueo: Un debate que no cesa.* Boletín del Ministerio de Justicia, 72 (2206), 2018, págs. 1-35.
- SILVA SÁNCHEZ, J. Mª. *Expansión del Derecho penal y blanqueo de capitales,* en *II Congreso sobre prevención y represión del blanqueo de dinero* (por ABEL SOUTO, M. y SÁNCHEZ STEWART, N.) Tirant lo Blanch, 2011, págs. 131-140.
- TENA PLATA, A. *Las criptodivisas y el blanqueo de capitales.* Universitat Jaume I, 2019, 59 págs.
- VEINTEMILLA CANDO, L. E. *Los activos criptográficos como objeto de un contrato de compraventa.* Universidad Católica de Santiago de Guayaquil. Ecuador, 2022, 39 págs.
- VERA RIVERA, Mª C. *El delito de administración desleal: criterios de política criminal, fundamentación del injusto y análisis de la tipicidad objetiva.* Madrid, 2017. 553 págs.

BIBLIOGRAFÍA COMPLEMENTARIA

- CADENAS, E., 2020. GAFI publica nuevos indicadores sobre criptomonedas para el blanqueo de capitales y financiación del terrorismo. En: *Cointelegraph* [en línea]. Disponible en: https://es.cointelegraph.com/news/fatf-publishes-new-indicators-on-cryptocurrencies-for-money-laundering-and-financing-of-terrorism [consulta: 26 de mayo de 2022.]

- CHAINALYSIS TEAM, 2022. Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume. En: *Chainalysis* [en línea] Disponible en: https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/ [consulta: 4 de septiembre de 2022.]
- CINCO DÍAS, 2022. La CNMV alerta de que suplantan su identidad en un intento de fraude con criptomonedas. En *CincoDías. El País Economía* [en línea]. Disponible en: https://cincodias.elpais.com/cincodias/2022/02/14/mercados/1644846982_270379.html [consulta: 20 de agosto de 2022.]
- CIVIETA, Ó., 2022: Japón será la primera gran economía mundial en regular las 'stablecoins', En: *Business Insider* [en línea]. Disponible en: https://www.businessinsider.es/japon-sera-primera-gran-potencia-regule-stablecoins-1071543 [consulta: 6 de junio de 2022.]
- DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO, 2018. Nota técnica sobre la gestión de fraude en operadores de juego. En: *Ministerio de Hacienda. Secretaría de Estado de Hacienda* [en línea]. Disponible en: https://www.ordenacionjuego.es/sites/ordenacionjuego.es/files/noticias/2018_12_20_nota_tecnica_de_gestion_de_fraude.pdf [consulta: 31 de agosto de 2022.]
- DSN, 2018. Desarticulada una organización criminal dedicada al blanqueo de capitales procedente del tráfico de drogas, haciendo uso de moneda virtual (criptomonedas). En *Departamento de Seguridad Nacional, Gobierno de España* [en línea]. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/desarticulada-una-organizaci%C3%B3n-criminal-dedicada-al-blanqueo-capitales [consulta: 30 de agosto de 2022.]
- EFE, 2007. Los 'paraísos informáticos', la mayor pesadilla de los 'ciberpolicías'. En: *El Mundo* [en línea]. Disponible en: https://www.elmundo.es/navegante/2007/10/22/tecnologia/1193064956.html [consulta: 26 de mayo de 2022.]
- EFF (s.f.) Acerca de EFF. En: *EFF* [en línea] Disponible en: https://www.eff.org/es/pages/acerca-de-eff [consulta: 4 de septiembre de 2022.]
- ESCRIBANO, M., 2022. La 'coctelera' cripto que EEUU persigue y puede marcar el futuro del sector. En: *El Confidencial* [en línea]. Disponible en:

https://www.elconfidencial.com/tecnologia/2022-09-05/tornado-cash-mezclador-criptomonedas-arrestos_3483897/ [consulta: 6 de septiembre de 2022.]

- EUROPOL, 2017. *Serious and Organised Crime Threat Assessment: Crime in the age of technology.* En: *EUROPOL* [en línea]. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/socta2017_0.pdf [consulta: 18 de agosto de 2022.]
- FROEHLINGSORF, J., 2022. Criptomonedas: del delito de estafa al blanqueo de capitales. En *CincoDías. El País Economía* [en línea]. Disponible en: https://cincodias.elpais.com/cincodias/2022/06/22/legal/1655914425_833391.html [consulta: 26 de mayo de 2022.]
- G. GARCÍA, J., 2020. Cajeros y casas de juego online, el refugio del blanqueo con criptomonedas. En *El País* [en línea]. Disponible en: https://elpais.com/tecnologia/2020-09-07/cajeros-y-casas-de-juego-online-el-refugio-del-blanqueo-con-criptomonedas.html [consulta: 18 de agosto de 2022.]
- GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, (s.f.). Money Laundering. En: *TAFT-GAFI* [en línea] Disponible en: https://www.fatf-gafi.org/faq/moneylaundering/ [consulta: 7 de mayo de 2022.]
- GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, (s.f.). Who we are. En: *TAFT-GAFI* [en línea] Disponible en https://www.fatf-gafi.org/about/whoweare/ [consulta: 7 de mayo de 2022.]
- GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, 2020. Informe sobre monedas virtuales: Definiciones claves y riesgos potenciales de lavado de activos y financiación del terrorismo. En: *TAFT-GAFI* [en línea] Disponible en: https://www.fatf-gafi.org/media/fatf/content/GAFILAT-Spanish-Virtual%20Assets-Red%20Flag%20Indicators.pdf [consulta: 7 de mayo de 2022.]
- LÓPEZ-FONSECA, Ó, 2019. Cae una banda que blanqueó 9 millones en tres meses con cajeros de criptomonedas. En: *EL PAÍS* [en línea]. Disponible en: https://elpais.com/economia/2019/05/08/actualidad/1557304294_288457.html [consulta: 4 de septiembre de 2022.]
- MIRANDA, D., 2022. ¿Qué son las criptomonedas y cómo funcionan? En: *National Geographic España* [en línea]. Disponible en:

https://www.nationalgeographic.com.es/mundo-ng/que-son-criptomonedas-y-como-funcionan_16981 [consulta: 28 de julio de 2022.]

- NELSON, J., 2022. ¿Qué son los mezcladores de criptomonedas y cómo funcionan? En *Decrypt* [en línea]. Disponible en: https://decrypt.co/es/resources/que-son-mezcladores-de-criptomonedas [consulta: 6 de septiembre de 2022.]
- PÉREZ, E., 2019. De Silk Road a la operación "Kampuzo": las incautaciones de criptomonedas más importantes para perseguir al crimen organizado. En *Xataka* [en línea]. Disponible en: https://www.xataka.com/criptomonedas/silk-road-a-operacion-kampuzo-incautaciones-criptomonedas-importantes-para-perseguir-al-crimen-organizado [consulta: 6 de septiembre de 2022.]
- POZZI, S., 2015. El fundador de Silk Road, condenado a cadena perpetua. En: *El País* [en línea]. Disponible en: https://elpais.com/internacional/2015/05/29/actualidad/1432935074_571369.html [consulta: 6 de septiembre de 2022.]
- PricewaterhouseCoopers, 2015. Prevención de la legitimación de capitales y financiamiento al terrorismo, conceptos, riesgos y sistemas de información. En: *Boletín de Consultoría Gerencial* [en línea] Disponible en: https://www.linkedin.com/pulse/pwc-prevenci%C3%B3n-de-legitimaci%C3%B3n-capitales-y-al-riesgos-montes-jimenez/?trk=articles_directory&originalSubdomain=es [consulta: 28 de julio de 2022.]
- VELASCO NÚÑEZ, E., 2021. Jurisprudencia de tribunales penales sobre blockchain y su aplicación a las criptomonedas. En *h50* [en línea]. Disponible en: https://www.h50.es/jurisprudencia-de-tribunales-penales-sobre-blockchain-y-su-aplicacion-a-las-criptomonedas/ [consulta: 28 de julio de 2022.]

LEGISLACIÓN CITADA

- Convenio de Budapest, de 23 de noviembre de 2001.
- Ley 13/2011, de 27 de mayo, de regulación del juego.
- Ley 21/2011, de 26 de julio, de dinero electrónico.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al mercado de los criptoactivos y por el que se modifica la Directiva (UE) 2019/1937.
- Real Decreto-ley 7/2021, de 27 de abril, de trasposición de directivas de la Unión Europea en las materias de competencia, prevención de blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

JURISPRUDENCIA REFERENCIADA

- Acuerdo del 3 de febrero de 2005 sobre el principio de ubicuidad por la Sala Segunda del Tribunal Supremo.
- Auto de la Sala Segunda del Tribunal Supremo, 21 de octubre de 2015. Número de recurso 20555/2015.
- Dictamen del Comité Económico, V. DIRECTIVA 2005/60/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de octubre de 2005 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.
- Resolución Vinculante de Dirección General de Tributos, V1029-15 de 30 de marzo de 2015.
- Sentencia del Tribunal de Justicia de la Unión Europea, de 22 de octubre de 2015, Skatteverket y David Hedqvist, asunto C 264/14 (ECLI:EU:C:2015:718).
- Sentencia del Tribunal Supremo 1013/2014, de 11 de marzo de 2014.
- Sentencia del Tribunal Supremo 1080/2010, de 20 de octubre de 2010.
- Sentencias del Tribunal Supremo 2019/2019, de 20 de junio de 2019.
- Sentencia del Tribunal Supremo 265/2015, de 29 de abril de 2015.
- Sentencia del Tribunal Supremo 326/2018, de 20 de junio de 2019.
- Sentencia del Tribunal Supremo 3504/2019, de 04 de noviembre de 2019.
- Sentencia del Tribunal Supremo 9965/2001, de 18 de diciembre de 2001.

Listado de abreviaturas, acrónimos y siglas.

- ATS: Auto del Tribunal Supremo.
- BBC: *British Broadcasting Corporation.*
- BCE: Banco Central Europeo.
- BCH: *Bitcoin Cash* (protocolo).
- BTC: *Bitcoin* (protocolo).
- CEO: *Chief Executive Officer.*
- CNMV: Comisión Nacional del Mercado de Valores.
- CP: Código Penal.
- DGOJ: Dirección General de Ordenación del Juego.
- DLT: *distributed ledger technology,* tecnologías de libro mayor distribuido.
- EFF: *Electronic Frontier Foundation.*
- ETH: *Ether* (protocolo).
- FBI: *Federal Bureau of Investigation;* Buró Federal de Investigaciones.
- GAFI: Grupo de Acción Financiera Internacional.

- IOTA: *Internet of Things* (protocolo).

- IP: Protocolo de Internet.

- LTC: *Litecoin* (protocolo).

- MiCA: *Market in Crypto Assets.*

- NFT: *Non fungible token,* token no fungible.

- OCU: Unidad Central Operativa de la Guardia Civil.

- ORGA: Oficina de Recuperación y Gestión de Archivos.

- PwC: *PricewaterhouseCoopers.*

- QR: *Quick Response.*

- SEPBLAC: Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

- STS: Sentencia del Tribunal Supremo.

- TJUE: Tribunal de Justicia de la Unión Europea.

- TS: Tribunal Supremo.

- UIF: Unidad de Inteligencia Financiera.

- XLM: *Stellar* (protocolo).

Anexos.

ANEXO A. Gráfico de incremento del uso fraudulento de los mezcladores de criptomonedas.

El siguiente gráfico representa la variación del volumen que se envía a los mezcladores de criptomonedas desde direcciones ilícitas, con categorización por colores de las distintas actividades de las que proceden los fondos. Los datos ofrecidos por Chainalysis se valoran trimestralmente.

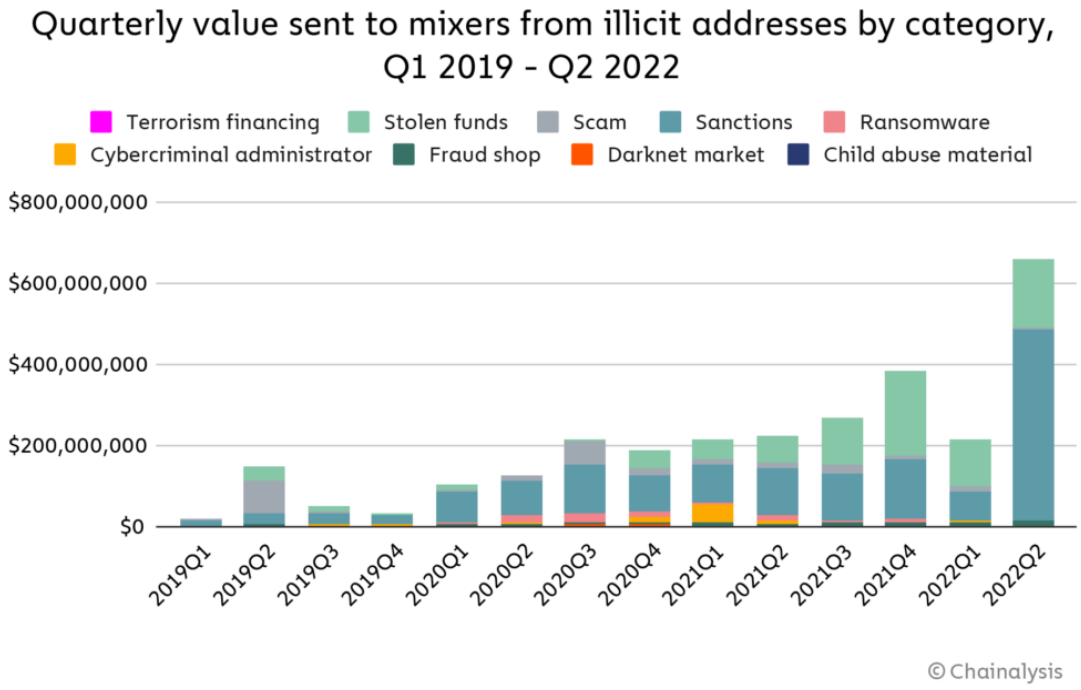

Imagen de Chainalysis.