Revista de Estudios Europeos
Publicación del Instituto Universitario de Estudios Europeos de la Universidad de Valladolid
EDICIONES Universidad Valladolid

El embargo y decomiso de criptomonedas en el Espacio Judicial Europeo*

Seizure and confiscation of cryptocurrencies in the European Judicial Area

JUAN JOSÉ NAVAS BLANQUEZ
Magistrado del Juzgado de Instrucción n.º 4 de Torremolinos.
jj.navas@poderjudicial.es
Recibido: 30/10/2022. Aceptado:30/11/2022.

DOI: https://doi.org/10.24197/ree.Extraordinario%20monogr%C3%A1fico%201.2023.349-383

Resumen: El auge en el uso de las denominadas TICs ha ocasionado importantes avances en nuestra sociedad, pero, a su vez, ha generado un incremento alarmante en la comisión de nuevos delitos en el ciberespacio adquiriendo un especial protagonismo el uso de criptomonedas. Uno de los grandes retos que se plantean a nivel jurídico es la forma de, primero, incautar y, posteriormente, decomisar las monedas virtuales utilizadas de forma ilícita en el seno de organizaciones criminales. El objetivo del presente estudio es ofrecer una visión global del cuál es el régimen jurídico de las criptomonedas y su incidencia en el proceso penal.
Palabras clave: Criptoactivos; Criptomonedas; Bitcoin; *Blockchain*; Ciberespacio; Embargo de monedero electrónico; Clave pública; Clave privada; Decomiso de criptomonedas.

Abstract: The boom in the use of so-called ICTs has caused important advances in our society, but, in turn, has generated an alarming increase in the commission of new crimes in cyberspace, acquiring a special role the use of cryptocurrencies. One of the great challenges that arise at the legal level is how to first seize and subsequently confiscate virtual currencies used illicitly within criminal organizations. The objective of this study is to offer a global vision of what is the legal regime of cryptocurrencies and their impact on the criminal process.
Keywords: Cryptoassets; Cryptocurrencies; Bitcoin; Blockchain; Cyberspace; Seizure of electronic purse; Public key; Private key; Confiscation of cryptocurrencies.

* Este artículo es resultado del Proyecto de investigación concedido por el Ministerio de Ciencia e Innovación titulado: "*Proceso penal y Unión Europea. Análisis y propuestas*" –PID2020-116848GB-100-, de cuyo equipo de trabajo forma parte el autor.

INTRODUCCIÓN

Uno de los grandes retos que desde de la Unión Europea se afrontan en la actualidad es paralizar las consecuencias negativas que supone la delincuencia organizada[1] y, muy especialmente, el impacto degenerativo que supone para las economías de los Estados miembros. Como alerta Europol en su informe de 12 de abril de 2021[2] hay grupos de criminalidad organizada estructurados en grupos perfectamente jerárquicos y multifuncionales dificultando desde el primer momento de la investigación la actuación policial a la hora de intentar el desmantelamiento de estas organizaciones. Esta situación ha provocado con el paso del tiempo una conciencia generalizada a todos los niveles de lo erróneo que puede resultar

un planteamiento focalizado en los clásicos planteamientos de justicia retributiva o, al menos, exclusivamente punitiva para girar hacia un enfoque mucho más pragmático en el que el fundamento a considerar es que sin dinero[3], cualquiera que sea su origen, las redes de actuación de este tipo delincuencia resultan más complicadas. Es en este punto, donde la UE ha incluido de forma progresiva en su hoja de ruta[4] una política criminal basada en que el delito no resulte beneficioso para quien lo cometa.

Fruto de este énfasis en la agenda programática de la UE es el resultado de una actividad legislativa[5], casi frenética, dando la sensación

---

[1] En mayo de 2021, el Consejo de la UE adoptó sus prioridades para la lucha contra delincuencia grave y organizada durante los cuatro años siguientes. Las prioridades se aplicarán entre 2022 y 2025 en el marco de la Plataforma Multidisciplinar Europea contra las Amenazas Delictivas (EMPACT).

[2] Informe Europol, 2021 European Union Serious and Organised Crime Threat Assessment (EU SOCTA). El informe íntegro se puede comprobar en: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime- threat-assessment.

[3] Sobre esta materia resulta muy ilustrativa la Comunicación de la Comisión sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025 al señalar que las organizaciones delictivas utilizan medios sofisticados para blanquear sus ingentes ingresos con una estimación al menos de 139 000 millones de euros al año.

[4] Véase en este sentido el Programa de Estocolmo: *Una Europa abierta y segura que sirva y proteja al ciudadano* (DOUCE C 115/01, 4/05/2010).

[5] Dentro de la actividad de la UE contra la Delincuencia Organizada (2021-2025), se encuentra la Propuesta de Directiva del Parlamento Europeo sobre recuperación de activos y decomiso de 25/05/2022, COM/2022/245 final, que busca como principal objetivo "*reforzar las capacidades de las autoridades competentes de identificar, embargar y gestionar activo así como las capacidades de decomiso a fin de que*

de que la principal prioridad, por no decir la única, es la lucha por revertir las ganancias ilícitas derivadas del delito a las arcas públicas, olvidando que sólo con un proceso de armonización en el Espacio Judicial Europeo tanto en las normas procesales como en las sustantivas de los Estados miembros es posible conseguir resultados satisfactorios y, lo más importante, erradicar o al menos mitigar, un fenómeno cada vez más extendido como es el de la delincuencia internacional organizada. Aunque no se trata de un problema nuevo[6], asistimos a la proliferación de un nuevo tipo de delincuencia que se aparta, hasta cierto punto, del concepto tradicional basado en la existencia de estructuras jerarquizadas localizables en distintos puntos de la geografía mundial.

Hoy en día, la criminalidad internacional es percibida a nivel policial como un negocio empresarial[7] cuyos objetivos son la obtención rápida de activos ilícitos, empleando para ellos una variedad de instrumentos no detectables o de difícil captación por los investigadores aprovechando el innegable proceso de globalización[8] al que asistimos. Entre estas herramientas, junto con la denominada ingeniería financiera se encuentra internet o, de forma más genérica, las Tecnologías de la Información y el Conocimiento-en adelante TICs-. Los avances informáticos, siempre en constante evolución, unido al desarrollo en las formas tradicionales de transacción económica, han favorecido la comisión de delitos a través de técnicas digitales en el denominado *ciberespacio*[9]. Por lo tanto, en esta primera aproximación de lo que representa las criptomonedas, resulta necesario tener claro una premisa básica: las TICs han supuesto una verdadera revolución mundial de la que se han visto beneficiadas millones de personas, pero, a su vez, han generado, como contrapartida, un nuevo

comprendan todas las actividades delictivas pertinentes llevadas a cabo por grupos de delincuencia organizada y permitan así decomisar todos los activos correspondientes."

[6] La problemática e incidencia en los intereses económicos de la UE del crimen organizado fue debidamente abordada en el informe del Parlamento Europeo sobre la delincuencia organizada en la Unión Europea, de 25 de octubre de 2011.

[7] Edwards, A y Gill, P. (2002): *¿El crimen como empresa? El caso del delito transnacional organizado".*Crime, Law and Social Change.

[8] Rubert P (2009), "*Globalización y delincuencia: el crimen organizado transnacional-. Actores no estatales y seguridad internacional*. Plaza y Valdés.

[9] Véase en este sentido el informe de Europol de 7 de diciembre de 2021 sobre los riesgos de la ciberdelincuencia cuyo contenido íntegro se encuentra en https://www.europol.europa.eu/publications-events/main-reports/iocta-reporten.

tipo de delincuencia mucho más sutil, volátil e, incluso, perniciosa a todos los niveles: *el cibercrimen*[10].

Partiendo de las anteriores consideraciones, con el presente trabajo me propongo analizar la incidencia del uso de criptomonedas en el entorno del ciberespacio y cómo se ha convertido en instrumento para potenciar la acumulación de activos patrimoniales de procedencia delictiva. Para ello me centraré especialmente, por los motivos que se indicarán, en el uso del bitcoin, tanto en lo relativo a su conceptualización como a su discutida naturaleza jurídica, detallando finalmente, las dificultades que acarrea el proceso de aprehensión de dicha moneda en las distintas fases del proceso penal.

1. RÉGIMEN JURÍDICO DE LAS CRIPTOMONEDAS: UNA BREVE APROXIMACIÓN A SU ACTUAL REGULACIÓN

Antes de adentrarnos en aspectos de índole práctico, conviene tener presente algunas cuestiones introductorias para asimilar adecuadamente el régimen legal de las criptomonedas. No pretendemos con ello ahondar en exceso en una materia ya de por sí compleja por su dificultad técnica, pero sí trazar algunas líneas básicas que permitan asimilar lo necesario para dar una respuesta jurídica al uso ilícito que de este tipo de moneda se está realizando en la actualidad.

1. 1. Algunas precisiones de tipo terminológico

1.1.1. ¿Qué son los criptoactivos?

Lo primero que llama la atención es la ausencia de una norma que regule los criptoactivos. De hecho, fruto de la necesidad de crear un bloque legislativo armonizado[11], la Comisión fijó dentro de la agenda denominada

[10] Según las estimaciones de la Comisión Europea enmarcada dentro del ámbito de la Resolución del Parlamento Europeo, de 10 de junio, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital costo de la ciberdelincuencia para la economía global en el año 2020 fue de 5,5 billones de euros

[11] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité Europeo de las Regiones por la que se establece el "*Plan de Acción en materia de Tecnología Financiera*." Bruselas, 08.03.2018 COM/2018/0109 final.

"Estrategia de Finanzas Digitales"[12] la necesidad de asegurar un marco normativo que asegure una respuesta común entre los Estados miembros, evitando la fragmentación y potenciando la seguridad jurídica. Consecuencia del anterior planteamiento es la propuesta de *Reglamento relativa a los mercados de criptoativos*[13]-en adelante Reglamento MICA- que por vez primera define lo que es un criptoactivo como "*una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar*."[14]

Reconociendo cierta ambigüedad de tipo conceptual, la anterior definición acoge lo que ya señalaban, tanto la Autoridad Bancaria Europea-en adelante EBA-, como la Autoridad Europea de Valores y Mercados-en adelante ESMA- en su informe de 9 de enero de 2019[15], esto es, que nos encontramos ante un *activo digital* que se caracteriza por encontrarse distribuido y registrado mediante el sistema de criptografía[16], ser utilizado como medio de intercambio o pago, con fines de inversión, para acceder a un producto o servicio, o bien una combinación de los anteriores y, finalmente, no encontrarse garantizado por un banco central o una autoridad pública. A la espera de la definitiva publicación del Reglamento MICA, los riesgos del uso incontrolado de criptoactivos son evidentes, incrementados especialmente a raíz de la crisis mundial del COVID-19[17], lo que ha llamado la atención de las autoridades de

[12] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Estrategia de Finanzas Digitales para la UE". Bruselas, 24.09.2020. COM (2020) 591 final.

[13] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. COM/2020/593 final.

[14] Art. 3.1.2 del Reglamento MICA.

[15] Informe de ESMA "Un asesoramiento dirigido a las instituciones de la Unión Europea sobre la Initial Coin Offering (ICOs) y criptoactivos. París, enero de 2019. El texto íntegro se encuentra en https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[16] Para el desarrollo de esta criptografía se utiliza la tecnología DLT (Distribuited Ledger Technology).

[17] La Disposición final segunda del Real Decreto-ley 5/2021, de 12 de marzo, de medidas extraordinarias de apoyo a la solvencia empresarial en respuesta a la pandemia de la COVID-19, asume los riesgos que representa la inversión de criptomonedas habilitando a la CNMV el control de la publicidad de criptoactivos.

supervisión del sistema financiero[18] con la finalidad de poner freno a eventuales prácticas abusivas.

Por lo tanto, en esta primera aproximación al término, podríamos concluir que los criptoactivos aglutinan todos los posibles tipos de activos digitales que ofrece el mercado financiero, pudiendo adoptar modalidades diversas, como títulos, monedas virtuales, efectos, bonos, participación siempre y cuando reúna las tres características indicadas anteriormente.

1.1.2. ¿Qué tipo criptoactivos existen?

La clasificación que más consenso genera es la que distingue entre dos tipos de criptoactivos: las criptomonedas y los tokens[19]. Aunque por razones obvias nos centraremos en la primera, es preciso explicar qué son los tokens.

Según la ESMA[20] "un *token* supone "*toda representación digital de un interés, que puede ser de valor, un derecho a recibir un beneficio o a desempeñar funciones específicas o puede no tener un propósito o uso específico*", mientras que el BCE[21] las considera como "*meras representaciones digitales de activos existentes que permiten registrar esos activos mediante una tecnología diferente*." De ambas definiciones nos interesa destacar que los tokens son una representación digital de bienes físicos, derechos u otros bienes que ofrecen a sus titulares créditos o derechos pero que, a diferencia de las criptomonedas, utilizan el sistema *blockchain*, sino que se encuentran reguladas por contratos inteligentes empleando la tecnología denominada como Distributed Ledger Technology[22].

---

[18] Comunicado conjunto del Banco España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos. Madrid. 17.03.21.

[19] Más ampliamente, GIL GIL, A y HERNANDEZ BERLINCHES, R (2019): *Cibercriminalidad.*Dykinson. Madrid.

[20] Así lo recoge en su informe titulado "*Advice on Initial Coins Offerings and Crypto-Assets*". Paris. 09.01.19. El texto íntegro se encuentra en https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[21] Informe del BCE «*Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*». Francfort. Mayo, 2019

[22] Tecnología de Contabilidad Distribuida (DLT) es empleada para almacenar y usar datos para ser utilizados en distintos lugares de la red y distribuidos entre los usuarios.

Por su parte, las *criptomonedas*, también denominadas monedas virtuales gozan, curiosamente, de unos cimientos conceptuales más asentados, quizás debido a que su uso se encuentra históricamente más generalizado dentro del comercio digital. Así, el art. 1 de la Directiva 2015/849, de 20 de mayo relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo define la moneda virtual "*como una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda de curso legal, que no tiene la consideración de moneda o divisa, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos."*[23]

Por tanto, ¿qué diferencia un token de una criptomoneda? En primer lugar,mn el uso de la tecnología, ya que las criptomonedas se basan en el sistema de encriptado *blockchain.* Sin embargo, existen otras dos características igualmente diferenciadoras:

.- Bajo un punto de *vista funcional*, los tokens incorporan más derechos que las criptomonedas. Desde esta perspectiva podríamos distinguir entre: *security tokens*, vinculados a activos financieros intercambiables como bonos, swaps, es decir, más próximos a lo que son las acciones tradicionales, y utility *tokens que* otorgan a sus titulares un derecho prioritario sobre el acceso a un producto o servicio[24], más próximos, por tanto, a las formas tradicionales de adquirir financiación.

.- Desde el punto de vista de la *finalidad* perseguida, las criptomonedas aspiran a convertirse en una alternativa a la moneda tradicional, llegando incluso asumir las funciones generalmente atribuidas al dinero[25].

[23] Esta definición ya fue en su momento acogida por el GAFI (Grupo de Acción Financiera Internacional.) en su informe "Monedas Virtuales: directrices para un enfoque basado en riesgo". Junio, 2015.

[24] Véase NAVARRO CARDOSO, F. (2019): "Criptomonedas (en especial, bitcoin) y blanqueo de dinero". *Revista Electrónica de Ciencia Penal y Criminología*, núm. 21-14, pp 31-33.

[25] Sobre esta cuestión, que no se puede abordar en este trabajo con más detenimiento, véase ROBLEH, A BARRDEAR, CLEWS. R y SOUTHGATE.J (2014): "The economics of digital currencies". Bank of England, *Quarterly Bulletin*, Q.3pp. 276 y ss..,

1.1.3. ¿Qué es la tecnología Blockchain?

La arquitectura tecnológica donde se genera todo el ecosistema que gira en torno a las criptomonedas se denomina *blockchain*. Es difícil encontrar una definición que aglutine el conjunto de características del sistema *blockchain* quizá, en parte, motivado por la ausencia clara de un regulador normativo o, simplemente, por la complejidad que supone entender esta tecnología.

Aun así, representa como indica VELASCO[26] "*un sistema distribuido de registros contables entre iguales que usa el algoritmo que negocia la información contenida en esos registros en bloque de datos ordenados*". Lo que caracteriza a este sistema criptográfico es la composición de bloques, es decir, una vez se cierra uno, aproximadamente cada diez minutos, se genera otro y todo ello a través del sistema de minado[27].

Realizando un paralelismo con lo que representa en el proceso penal la investigación de cuentas o el análisis financieros de documentos, lo que genera el b*lockchain* según indica muy gráficamente ARÁNGUEZ SANCHEZ[28] es "*un gran libro virtual de contabilidad*", una gran base de datos, donde ningún asiento se puede borrar o modificar y que no la gestiona una sola persona, sino muchas, haciendo un asiento. En este gran libro, todas las transacciones se agrupan en bloques, que se van añadiendo de forma sucesiva al libro registro[29]. El eslabón que une los bloques es lo

[26] VELASCO NUÑEZ, E. (2020): "Aspecto jurídico penales vinculados al *blockchain* y las criptomonedas: delito fiscal, blanqueo de capitales, robo, estafa.", artículo monográfico publicado en SEPIN en enero de 2020, pp.1 y ss.

[27] El proceso de minado es aquel empleado para validar las transacciones realizadas en la red para ser agregadas a la base de datos de la *blockchain*. Esta actividad es realizada por los mineros que, a cambio, obtienen una comisión o recompensa.

[28] ARANGUEZ SANCHEZ, C (2020). "EL bitcoin como instrumento y objeto de delitos". *Cuadernos de Política Criminal*, núm.131, pp.82 y ss.

[29] Para entender mejor lo que como funciona el *Blockchain*, resulta muy ilustrativo el siguiente ejemplo: "A propondrá una transacción al resto de los nodos, consistente en que dos BTC registrados en su cuenta pasen a estar registrados en la cuenta de B y se eliminen de la suya. El mensaje de A incluirá (i) la cantidad de BTC a transferir (aquí, 2) y (ii) la dirección a la que se transferirán (cuenta de B). 2. El mensaje con la transacción propuesta será recibido de forma encriptada por los nodos validadores, que verificarán (i) que la proposición de transacción ha sido enviada por el usuario que debe transferir los BTC (en nuestro caso, por A), (ii) que el usuario dispone de la cantidad de BTC que desea transmitir y (iii) que el usuario destinatario existe. 3. Si el mensaje de A es correcto, los nodos validadores calcularán su hash 12. El hash,equiparable a una huella dactilar o

que se denomina "hash", que no deja de ser un algoritmo matemático generado aleatoriamente, cuya solución compete a los conocidos como mineros cuyo objetivo, en definitiva, es alcanzar la solución de un problema matemático que genera precisamente la criptomoneda.

De lo que es el *blockchain*, al menos en lo que nos interesa en este trabajo, se destacarían las tres siguientes características:

- Se basa en un sistema d*escentralizado.* A diferencia de lo que pudiera ocurrir por ejemplo en una transferencia de dinero en un banco, no existe intermediación por una autoridad supervisora, siendo las partes o nodos[30] las únicas que forman parte del proceso de transacción, poniéndolos a todos en pie de igualdad.

- *Inmutabilidad e irrevocabilidad de la operación*, ya que desde el mismo momento en que es configurada en la red, el sistema criptográfico impide que pueda ser variada o revertida la transacción realizada. Esta característica se antoja esencial a la hora de averiguar las posibles transacciones ilícitas de criptomonedas por parte de la policía. Al no existir terceros que validen la operación, la cadena no puede ser alterada o modificada permaneciendo inalterable.

---

elemento específico de cada transacción, permite identificar una transacción de forma individualizada, puesto que se obtiene a partir de su concreto contenido y es único13. 4. La transacción verificada se incluirá en un bloque, es decir, en un paquete de información que contiene las últimas transacciones recibidas y verificadas en un determinado lapso de tiempo. Cada bloque incluye: a. el hash del bloque anterior; b. el hash raíz: el hash resultante de aplicar el algoritmo al conjunto de los hashes de todas las transacciones que integran el bloque; c. el sello temporal del bloque (i.e., día y hora en que el bloque se ha aprobado); y d. el hash del propio bloque: aplicar la función hash al conjunto de (a, b y c). 5. Antes de poder «cerrar el bloque» e incluirlo en la cadena, el nodo validador realiza cálculos para resolver un problema matemático consistente en hallar una combinación numérica (el llamado nonce), que debe colocarse al inicio del hash y que solamente puede ser resuelto mediante prueba y repetición14. 6. La nueva versión del libro registro es remitida a todos los nodos". PORXAS, N y CONEJERO, M, (2018). "Tecnología Blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados. *Actualidad jurídica Uría Menéndez*. Num.48, p.27.

[30] Los nodos son la parte esencial en la tecnología Blockchain y aunque con muchas matizaciones representarían en la red todos los ordenadores conectados a la red sobre la que se hace funcionar el software que sustenta la cadena de bloques.

- *Volatilidad*. Unos de los factores de riesgo asociado a las critpomonedas es, sin duda, que va asociado a un mercado altamente especulativo sin unos parámetros estables, o al menos seguros, lo que genera fuertes fluctuaciones, fomentando la inversión especulativa[31].

1.2. Las criptomonedas en el contexto de la cibercriminalidad

Definir con ciertas garantías lo que es la cibercriminalidad no es tarea fácil, principalmente por un aspecto al que hemos hecho referencia con anterioridad, la falta de armonización normativa conlleva el uso indiscriminado de términos, en muchas ocasiones confusos, tales como delitos informáticos, delitos cibernéticos o ciberdelitos. La definición que quizás genera más consenso, especialmente a nivel doctrinal[32], es aquella que equipara de forma casi minimalista el cibercrimen a aquellos supuestos en el que de forma directa o indirecta se ven involucrada las TICs, ya sea como *el objetivo o* como el *instrumento* de comisión[33] del delito. Lo que sin embargo no genera polémica alguna, como expresamente recalca Europol en su Informe IOCTA, de 13 de noviembre de 2021[34], es que a raíz de la crisis humanitaria provocada por la COVID 19, la ciberdelincuencia es cada vez más metódica a la par que agresiva, aumentado los ataques masivos a empresas y particulares, convirtiendo sus ganancias ilícitas en criptomonedas cuyo rastro digital es, en muchas ocasiones, difícil de detectar.

Por lo tanto, y antes de ahondar en la problemática actual del bitcoin, me propongo exponer de manera somera cuál es el actual marco legislativo en el ámbito de la ciberdelincuencia y de las criptomonedas.

Así, en el marco del Consejo de Europa, el *Convenio sobre la Ciberdelincuencia*, firmado en Budapest el de 23 de noviembre de 2001, supuso un importante avance en esta materia, buscando un doble objetivo: por un lado, aproximar las legislaciones penales nacional y permitir la

[31] ARANGUEZ SANCHEZ, C (2020). "EL bitcoin como instrumento y objeto de delitos". *Cuadernos de Política Criminal*, núm.131, p.80.

[32] Este tema es abordado con más detalle en MIRO LLINARES, F. and MONEVA, A. (2019). "What about cyberspace and cybercrime alongside it". *Crime Science*, num.8, pag.12 y ss.

[33] PEREZ MEDINA, D, "Blockchain, criptomonedas y los fenómenos delicitivos: entre el crimen y el desarrollo" (2020). *Boletín Criminológico*, núm.206, pp. 13-15.

[34] Informe sobre *Internet Organised Crime Threat Assement(IOCTA)*, adoptado el 13 de noviembre de 2021

utilización de medios eficaces en materia de delitos informáticos[35] y, por otro, establecer un mecanismo rápido de cooperación internacional contra la ciberdelincuencia[36]. Resulta evidente que la mutabilidad de este tipo de fenómeno delictivo deja al Convenio en un estado casi permanente de obsolescencia que necesitaría como mínimo una revisión prácticamente anual del texto normativo[37].

En el ámbito de la UE, sorprende, como mínimo, un bagaje legislativo hasta el momento ciertamente escaso, sin que se lleguen a determinar las bases conceptuales de lo que ha de entenderse como ciberdelincuencia, sin afrontar de forma global los sempiternos problemas que plantean este tipo investigaciones, enrocados, en multitud de ocasiones, en conflictos jurisdiccionales y, sobre todo, en las dificultades en la obtención transfronteriza de pruebas digitales. A pesar de ello, se han ido consiguiendo ciertos logros dignos de ser mencionados.

En esta línea, las "*Conclusiones sobre la mejora de la justicia penal en el ciberespacio de 2016*[38]*,* el Consejo de la UE estableció una hoja de ruta[39] con la finalidad de mejorar los procedimientos de asistencia judicial, de cooperación con los proveedores de servicios y los problemas de jurisdicción. De hecho, el Consejo y la Comisión elaboraron las conclusiones tituladas *"Resiliencia, disuasión y defensa: fortalecer la ciberseguridad*, de 20 de noviembre de 2017[40], indicando, entre otras medidas, una propuesta de Reglamento sobre las ordenes europeas de

[35] De conformidad con la Resolución 1º, adoptada por los Ministros de Justicia europeos, en sus XXI Conferencia (Praga, 10 y 11 de junio)

[36]De conformidad con la Resolución 1º, adoptada por los Ministros de Justicia europeos, en sus XXI Conferencia (Praga, 10 y 11 de junio)

[37] Actualmente junto con el Convenio de Budapest se han firmado dos protocolos: el Protocolo adicional respecto de la criminalización de actos de naturaleza racista y xenofóbicos cometidos a través de sistemas de ordenador de 2003 y el Segundo Protocolo adicional relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas aprobado por el Comité de ministros el 17 de noviembre de 2021 y firmado por España el 12 de mayo de 2022.

[38] Documento del Consejo de la Unión Europea publicado en Luxemburgo el 9 de junio de 2016 con el número. 7371/16.

[39] La Séptima ronda de evaluaciones mutuas sobre "*Implementación y aplicación práctica de las políticas UE para la prevención y lucha contra el cibercrimen»* terminó en 2017 y fue sometido a evaluación al Consejo el 12 y 13 de octubre de 2017.

[40] Comunicación conjunta al Parlamento Europeo y al Consejo, de 13 de septiembre de 2017, Resilencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. JOIN(2017) 450 final

entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[41]. Este instrumento junto con el Reglamento 2021/784, de 29 de abril de 2021, sobre la *lucha contra la difusión de contenidos terroristas en línea*[42] y la Directiva 2014/41/CE, de 3 de abril de 2014 relativa a la *Orden Europea de Investigación* en materia penal[43] han de sentar las bases de la futura lucha contra la ciberdelincuencia en todas sus facetas.

Vemos por lo tanto que, a la espera de lo que puedan significar en la práctica estos instrumentos normativos, más focalizados, quizás en aspectos procesales de la investigación, el otro gran reto es combatir la utilización fraudulenta de criptomonedas y más concretamente d*el bitcoin,* cuya esencia, como expondremos, se nutre de las características propias de la ciberdelincuencia.

Por todo, la UE ha ido asentado de forma paulatina las bases normativas con la esperanza puesta en poner freno al empleo, cada vez más generalizado, de criptoactivos como forma clandestina de realizar transacciones económicas de cualquier índole aprovechando el anonimato que generan las TICs[44]. A tal fin, se acordó la *Resolución del Parlamento Europeo, de 26 de mayo de 2016 sobre monedas virtuales*[45] que, entre otros objetivos busca implementar "*un marco jurídico sólido que esté a la altura de la innovación, garantizando una respuesta oportuna y proporcionada".*

Fruto de esta necesidad, casi imperiosa, de robustecer el sistema legislativo, se publicó la *Directiva 2018/843, de 30 de marzo, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la*

[41] Documento de la Comisión Europea pubicado en Estrasburgo el 17 de abril de 2018, COM(2018) 225 final.
[42]. Publicado en el DOUE el 17 de mayo de 2021.
[43] Publicado en el DOUE el 1 de mayo de 2014.
[44] Fruto de esta alarmante situación, Europol ha reseñado minuciosamente en su informe "*Criptomonedas:rastreando la evolución de las finanzas criminales*", cómo los criminales utilizan las criptomonedas como medio de pago en sus operaciones clandestinas, especialmente para blanquear activos ilícitos, constituyendo uno de los grandes retos de los investigadores. Luxemburgo, Diciembre 2021. El informe íntegro se puede consultar en la siguiente dirección: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.
[45] Publicado en el DUOE el 28 de febrero de 2018.

financiación del terrorismo[46] que, aunque en un ámbito muy concreto, el blanqueo de capitales, supone la primera vez en la se fijan unas pautas para controlar el uso de la moneda virtual, convirtiendo a los proveedores de monederos electrónicos y a las plataformas de intercambio entre moneda virtual y fiduciaria en sujetos obligados al amparo de la Ley 10/2010, de 28 de abril de prevención del blanqueo de capitales y la financiación del terrorismo..

Por último, cabe destacar dos importantes iniciativas legislativas, aún pendientes de su definitiva publicación, pero que responden a la ya anunciada política de la Comisión de apuntalar la regulación jurídico-financiera de las criptoactivos. En primer lugar, la propuesta de *Reglamento relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos*[47], que supone una modificación del Reglamento 2015/847, de 20 de mayo de 2015[48], ampliando a los criptoactivos los requisitos de trazabilidad e información que se aplican a las transferencias electrónica. Por otro lado, la Comisión aprobó en septiembre de 2020 el programa denominado *Digital Finance Package*, que incluye cuatro propuestas legislativas, destacando por su importancia en esta materia, la *Propuesta de Reglamento relativo al mercado de criptoactivos entre de regulación del mercado de* criptoactivos, conocida como propuesta MICA dando cobertura legal a los servicios relacionados con los criptoactivos.

1.3. Clases de criptomonedas: el Bitcoin

Resulta difícil evaluar el número de criptomonedas implantadas en el mercado, siendo la horquilla tan grande que oscilan entre las 500 evaluadas por el BCE[49] y las cerca de 10.000 que, según el portal CoinMarketCap, existen en la actualidad. Esta disparidad numérica puede ser debida a que

[46] Dicha Directiva modifica, a su vez, las Directivas 2009/138/CE y 2013/36/UE-

[47] Dicha propuesta se enmarca en el "*Plan de acción para una política global de la Unión en materia de prevención del blanqueo de capitales y de la financiación de terrorismo*", de 7 de mayo de 2020, publicado en el DUOE el 13 de mayo de 2020.

[48] Reglamento del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativo a la información que acompaña a las transferencias de fondos y por el que se deroga el Reglamento (CE) nº 1781/2006

[49] Informe del BCE "Virtual currency schemes-a futher analysis", pag.32, Francfort, Febrero de 2015. El informe se encuentra disponible en: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

la inmensa mayoría de ellas son prácticamente una copia de las otras, eso sí, con distintas denominaciones. Dentro de esta amplia variedad, las más conocidas junto con *Ether, Binance Coin, Liecoin, Rippley*, es el *Bitcoin* de la que haremos una pequeña referencia sobre su origen y funcionamiento.

No hay constancia de quien creo el bitcoin, salvo que fue puesta en funcionamiento por vez primera en el año 2009 por un ciudadano australiano bajo el seudónimo de "Satoshi Nakamoto" cuya verdadera identidad a día no ha sido revelada, aspirando a convertirse en un medio alternativo al pago tradicional entre usuarios, utilizando, para ello, la mencionada tecnología *blockchain.* Como indica VELASCO[50] el *bitcoin* es ante todo un "*sistema de efectivo electrónico"*, que emplea el registro de transacciones mediante las redes entre pares (P2P), ofreciendo una alternativa al dinero fiduciario.

Pero ¿qué hace tan atractivo el uso de bitcoin? Sin duda alguna, la ausencia de un soporte físico, su anonimato, la rapidez a la hora de realizar operaciones de una cuenta a otra sin intermediario y, sobre todo, su carácter descentralizado lo que generó en los últimos años unas enormes expectativas, aspirando a convertirse en un medio alternativo a la moneda fiduciaria. Como contrapartida a esta "euforia" inicial un tanto desmedida en el uso de bitcoin, la enorme fluctuación monetaria que ha ido generando y su gran volatilidad[51] ha provocado un cierto recelo a la hora de generar nuevos inversores, frenándose su adquisición en los últimos años.

1.4. Naturaleza jurídica

Gran parte de la controversia que gira en entorno a las criptomonedas se centra en el alcance de su naturaleza jurídico-penal, es decir, en concretar no tanto lo qué son sino, más bien, lo que representan en las operaciones que a diario se realizan en la red. El que las criptomonedas aspiren, como hemos indicado, a desempeñar en términos financieros un

[50] VELASCO NUÑEZ, E. (2020): "Aspecto jurídico penales vinculados al blockchain y las criptomonedas: delito fiscal, blanqueo de capitales, robo, estafa.", artículo monográfico, *Sepin*, Enero de 2020, pp.4.

[51] Según el portal económico Bloomberg el bitcoinn pasó de valer 1 dólar en abril de 2011 a los 29,6 dólares en junio de ese año, llegando a alcanzar en octubre de 2013 los 1137 doláres, con un máximo histórico en abril de 2021 de 64.000 dólares. Para medir la votalidad tan cambiante se crearon los índices BitVol y EthVol.

papel semejante al del dinero tradicional no significa, en modo alguno, que puedan ser consideradas dinero, al menos como siempre lo hemos concebido. La existencia de factores de riegos y la ausencia de una normativa clara han ocasionado un cierto recelo por parte de las autoridades supervisoras a equipar la moneda virtual a la moneda de curso legal, dejando bien claro que nos encontramos ante dos tipos de conceptos distintos, aunque en algún aspecto compartan elementos comunes.

Desde un primer momento la postura del BCE ha sido la de considerar a las criptomonedas como moneda fiduciaria-*fiat currency*[52]- al reunir tan sólo de forma parcial las tres características que tradicionalmente se entienden ha de tener cualquier divisa:

- servir como medio de cambio al contar con un nivel de aceptación ínfimo si lo comparamos con la totalidad de las transacciones monetarias que se realizan a nivel mundial.
- como unidad de cuenta dado lo fluctuante del precio generado en torno a los criptoactivos, lo que la convierte en una fuente indeseable de especulación y riesgo para posibles los inversores.
- depósito valor, esto es, que sea permanente y duradero en el tiempo que permita cierto ahorro, lo cual es difícilmente compatible con su volatilidad en el mercado.

Igualmente, la EBA[53] niega que sea moneda, haciendo hincapié, entre otros motivos, en que su carácter descentralizado le impide tener dicha consideración al no estar emitida por ninguna autoridad central que la supervise adecuadamente.

Sin embargo y a pesar de la "contundencia" con la que manifiestan estos organismos, la cuestión hoy en día no queda resuelta. Muestra de lo que nos referimos es que la Directiva 2018/843, de 20 de mayo, conocida como Quinta Directiva antiblanqueo, no sólo las define como "*moneda"* virtual, sino que, además, en su Considerando 10 les reconoce "*su uso frecuente como moneda de pago, como medio de cambio y como unidad de cuenta*".

[52] Informe del BCE "*Virtual currency schemes-a futher analysis*", pag.12, Francfort, febrero de 2015.

[53] EBA Opinion on "virtual currencies", pag 21, Paris, 4 de julio de 2014. El informe íntegro se puede consultar en: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

Por lo tanto, si no pueden ser en consideradas íntegramente como moneda de curso legal, pero, como vemos, en parte sí responden a las funciones tradicionales de la moneda *fiat* ¿qué naturaleza jurídica tienen? Como veremos, no es esta una cuestión fácil de responder, por lo que pasaremos a continuación a exponer las distintas soluciones, tanto legales como jurisprudenciales, que se han ofrecido hasta el momento.

En primer lugar, ya se encarga la V Directiva en el mencionado Considerando 10 aclarar que la moneda virtual "*no debe confundirse con el dinero electrónico, tal y como se define en el artículo 2, punto 2 de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo"*.[54] Efectivamente, el ejemplo más ilustrativo de dinero electrónico lo ofrece la aplicación Paypal que representa un sistema de pago que se realiza de forma digital, ya sea con tarjetas o monederos electrónicos, pero respaldado en una unidad monetaria y, por lo tanto, sometida a un proceso de control y centralización que no ocurre en el caso de las criptomonedas.

Igualmente, el Considerando 10 las excluye de ser admitidas como f*ondos* en el sentido establecido en el artículo 4, punto 25 de la Directiva 2015/2366[55] o como *valor monetario almacenado en instrumentos externos*, tal y como se especifica, también, en el artículo 3, letras k) y l) de la Directiva 2015/2366.

Tampoco a nivel jurisprudencial los escasos pronunciamientos en esta materia han resultado ser demasiado clarificadores.

En el ámbito del derecho europeo, la sentencia del *TJUE* de 22 de octubre de 2015, *Skatteverket c. David Hedqvist, asunto C-264/14*[56] es, por el momento, la única que trata la cuestión sobre qué tipo de relación jurídica aflora en la transacción de los bitcoins. La conclusión a la que llega el Tribunal es que la actividad de cambio de bitcoins por monedas de curso legal constituye "*una prestación de servicios a título oneroso*"

[54] La Directiva 2009/110/ CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2019 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades ha sido objeto de trasposición mediante la Ley 21/2011, de 26 de julio, de dinero electrónico.

[55] Directiva 2015/2366/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios en el mercado interior.

[56] La cuestión resolvió dos preguntas planteadas por el Tribunal Supremo sueco relativa a la interpretación que respecto a la Directiva 2006/112, de 28 de noviembre pudiera generar el uso de bicoins: si la actividad de cambio de bitcoins constituye una prestación de servicios a título onerosos y, en caso afirmativo, si estaría exenta o no del IVA según el artículo 135.1 de la mencionada Directiva.

quedando exenta del régimen de tributación del I.V.A al amparo de la Directiva 2006/112, de 28 de noviembre. Lo relevante de esta decisión, a nuestro juicio, no es tanto la conclusión a la que se llega, sino, más bien, su *ratio decidenci*, al entender que la finalidad del uso de bitcoin no es otro que la de ser "una *divisa virtual de flujo bidireccional, que se intercambia por divisas tradicionales en las operaciones de cambio, que no tiene ninguna finalidad distinta de la de ser un medio de pago*"[57]. Lo cierto es que esta sentencia choca con la postura del BCE o de la EBA, más partidarias de negar, como hemos advertido, que las criptomonedas sean moneda. Dejando al margen esta polémica, como indica PEREZ LOPEZ[58], el alcance de la sentencia del TJUE ha de ser valorada en su justa medida, al tratarse, primero, de un tipo específico de criptomonedas, los bitcoins, que no abarca la totalidad de las criptomonedas y, segundo, su ámbito de aplicación se ciñe a una norma comunitaria muy concreta, la Directiva 2006/1152, de 28 de noviembre relativa al sistema común del I.V.A.

Por lo que respecta a nuestro ordenamiento jurídico, la sentencia del *TS num.2109/2019, de 20 junio de 2019,* resultó mucho más contundente tras afirmar[59] que "*los bitcoins no son monedas de curso legal"* ya que no pueden ser considerados dinero tal y como es definido en el artículo 1. 2 de la ley 21/2011, de 26 de julio de dinero electrónico[60] . Aunque a este extremo nos referiremos con más detenimiento al tratar el decomiso y restitución de criptomonedas, la sentencia del TS, a diferencia de la del TJUE, sí se atreve a definir el bitcoin como "*activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología y criptografía denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en*

[57] Conclusión 24.

[58] PEREZ LOPEZ, X. (2017): "Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Revista de Derecho Penal y Criminología*, num. 18, julio de 2017, pag.148.

[59] Fundamento jurídico 3º.

[60] El artículo 1.2 de la Ley 21/2011, de 26 de julio, de dinero electrónico, define el dinero electrónico como "*el valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicio de pago y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico*."

la venta que de estas unidades se realiza a través de las plataforma de trading Bitcoin."[61]

Quizás la problemática generada en torno a la naturaleza jurídica de las criptomonedas venga dada por la ausencia, hasta cierto punto lógica si tenemos en cuenta su carácter novedoso, de unos consolidados asideros legislativos y jurisprudenciales. La equiparación de la criptomoneda a la moneda virtual, aún no siendo errónea, sí puede generar cierta confusión terminológica pues, de un lado, se la considera, al menos legislativamente, moneda virtual como medio de pago, pero por otro y de forma mayoritaria, se niega que sean dinero o divisa.

Pero entonces, desde la óptica del proceso penal, ¿qué consideración se le ha de dar a una criptomoneda? A nuestro juicio, no siendo dinero, pero desempeñando una función semejante, lo más acorde conforme el pronunciamiento del TS es entender que se trata de un activo económico, pero de naturaleza inmaterial e intangible y, como tal, entendemos que tendría mejor encaje fuera considerado como un "efecto judicial" al amparo del artículo 368 bis de la LECrim y, por lo tanto, susceptible de ser intervenido en el marco de cualquier tipo investigación penal[62].

2. EL PROCESO DE INCAUTACIÓN DE CRIPTOMONEDAS

La forma en que ha de llevarse a cabo la incautación de criptomonedas supone un largo y complicado proceso que, a falta de una normativa clara, proponemos que se estructure en las siguientes fases:

- Una primera, incipiente y de mayor recorrido, que podemos denominar *de localización,* centrada en averiguar tanto la *dirección pública* creada por el sujeto investigado como en conocer la *clave privada* que permita "acceder" al interior del monedero.

- Una segunda, centrada en la adopción de medidas cautelares que aseguren a través del *embargo* que la criptomoneda no pueda ser transferida de forma ilícita a terceras personas.

[61] Fundamento jurídico 3º

[62] Así ocurre cuando en el transcurso de una entrada y registro domiciliario se intervienen objetos de diversa índole relacionados con el delito, como por ejemplo ordenadores, tablets o teléfonos móviles, los cuales son posteriormente analizados por la unidad investigadora con supervisión del Juez de Instrucción.

.-Finalmente, en tercer lugar, el decomiso o, en su caso, restitución al perjudicado de la moneda virtual intervenida.

Veamos a continuación los aspectos más importantes de cada una de ellas:

2.1. La fase de localización

El gran problema que enfrentan los investigadores a la hora de concretar quién o quiénes se encuentran "detrás" de una *wallet* es el poder vincularla una persona física o jurídica, a diferencia de lo que ocurre, por ejemplo, con la averiguación de cuentas bancarias al solicitarse datos directamente al banco o consultar telemáticamente el *Fichero Titularidades Financieras*[63], obteniendo información casi actualizada del titular, cuentas vinculadas, movimientos efectuados o productos financieros contratados. Cuestión distinta es que esa información resulte definitiva, que normalmente no lo es, y se tenga que acudir a diligencias de investigación complementarias que acrediten al titular real de la cuenta. Debemos entonces preguntarnos ¿cómo se llega a la dirección pública de la *wallet* y, vinculado a lo anterior, cómo se obtiene la clave privada.?

- La localización de la dirección pública: las empresas *exchangers*.

El hecho de que las operaciones vinculadas a criptodivisas, como se ha explicado, sean anónimas o, mejor dicho, pseudoanonimas, no significan que no dejen un rastro o trazabilidad digital que permita conocer, tanto quien autoriza el envío de monedas como el destinatario final de la transacción. Ocurre, sin embargo, que a la hora de analizar estas operaciones la situación es mucho más compleja, al no existir una autoridad central que las supervise o respalde en caso de existir alguna irregularidad. No existiendo un "lugar" al que acudir para conocer cuáles fueron las condiciones en las que se creó virtualmente una cartera para la identificación de la dirección pública es necesario seguir máximas de experiencia, por lo que debemos distinguir dos supuestos:

[63] Creada por Orden ECC/2503/2014, de 29 de diciembre por el que se constituye el Fichero de Titularidades Financiera, publicado en el B.O.E de 31 de diciembre de 2014.

- Cuando existe una víctima plenamente identificada, tras haberse producido, por ejemplo, un movimiento no autorizado en criptomonedas fruto de una extorsión previa o una situación de engaño. En estos casos, para acceder a la dirección pública generada tras crear un *monedero*, bastaría en principio con seguir el rastro de la transacción no autorizada llevada a cabo desde la *wallet* de la víctima a la cuenta de destino donde se han enviado la moneda virtual. Esto no significa dar siempre con la dirección pública de quien comete el delito ya que esta última dirección a su vez se ha podido dirigir a otras tantas direcciones y de esta forma perderse la trazabilidad de forma definitiva.

- Cuando se tengan sospechas fundadas en el marco de una determinada investigación de que un sujeto u organización esté utilizando criptoactivos como medio de pago para la adquisición de mercancías ilícitas o, simplemente, para blanquear dinero. Aquí la situación es mucho más compleja, pues esa primera "pista" que ofrece el rastro de la transacción realizada por la víctima no existe. Para averiguar la dirección pública se tendría que acudir a las formas tradicionales de investigación de la fase de instrucción, especialmente aquellas medidas que afectan o limitan derechos fundamentales. La explicación es obvia, fruto de una actuación normalmente secreta y con supervisión de un Juez de Instrucción, algunas de estas diligencias de investigación como será, por ejemplo, el análisis de dispositivos informáticos incautados[64], permitirán conocer documentos, cuentas de correo electrónicos o datos almacenados en la red o subidos a sistemas remotos de almacenamiento.

Una vez obtenida la dirección pública, el obstáculo a solventar es cómo obtener todos los datos generados en la *walle*t y que permita vincularla a las personas sospechosas que "a priori" son las que han creado la cuenta. Siguiendo con el ejemplo anterior, obtenida la totalidad de los dígitos bancarios de una cuenta, a continuación, se requeriría al banco para conseguir toda la información posible.

[64] El supuesto característico es el que se recoge en el artículo 588 sexies de la Ley de Enjuiciamiento Criminal que permite con ocasión de una diligencia de entrada y registro de dispositivos informáticos intervenidos tanto dentro como fuera del domicilio de una persona.

Ahora bien, tal y como se ha expuesto, si una de las características de la tecnología *blockchain* es su carácter descentralizado ¿a qué "lugar" acudir una vez obtenida la dirección pública de la *wallet*?.

El siguiente paso en la estrategia policial se centra en los proveedores de servicios de monederos electrónicos que, a su vez, pueden ser de "*cambio de moneda virtual por moneda fiduciaria*" y "*de custodia de monederos electrónicos*"[65]. Las primeras son conocidas comúnmente como empresas *exchangers* cuyo funcionamiento se asemeja mucho a una especie de "mercado persa virtual" regido por las normas de la oferta y la demanda de criptomonedas. A su vez, este tipo de servicio pueden ser de dos tipos:

- *Exchangers descentralizadas* que son aquellas que no se encuentran intervenidas por ningún intermediario y, como indica QUESADA[66] "*funcionan de forma automatizadas mediante contratos digitales inteligentes-smart contracts- que firman las partes involucradas, a su vez almacenadas en el blockchain*." La problemática es evidente y supone un serio escollo en el proceso de investigación, al ser los propios particulares los que "gestionan" la transacción mediante la tecnología P2P o "peer to peer"[67]lo que dificulta conocer la identidad real de la persona que firma la operación. En estos casos, la principal vía de investigación se centrará en la averiguación de la dirección IP desde el equipo en el que se haya autorizado la transacción.

[65] El artículo 3 de la V Directiva define al "proveedor de servicios de custodia de monederos electrónicos" como "*una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales*."

[66] QUESADA LOPEZ, P.M (2021): "Breves notas sobre la investigación de delitos en la que intervengan criptomonedas" en *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*. Madrid. Capítulo 14, pag.8

[67] La red de comunicación Peer to Peer es un modo de comunicación descentralizado en la red que permite la libre comunicación dentre usuarios y a través de un software la descarga directa de archivos desde la red.

- *Exchangers centralizados*[68]. Aquí es la empresa, la que actúa como intermediaria en la operación entre los particulares, a cambio de una determinada comisión, controlando la entrada y salida de fondos.

Como es obvio, debemos centrarnos en ésta últimas ya que, al estar supervisadas materialmente por un tercero, pueden aportar datos muy valiosos para la investigación como los nombres de quien creo la cuenta, correos electrónicos, domicilios o números de teléfonos, cuentas bancarias, en definitiva, lo que se busca es identificar plenamente al usuario para poder validar las transacciones que se hayan podido realizar[69]. Esta información es aportada al proceso penal tras un requerimiento directo de la unidad de investigación policial al proveedor de servicio en un modelo normalizado en inglés denominado "*A template of Law Enforcemente request por VC facilited crimes*", en el que se concreta, entre otros aspectos, tanto el objeto de la investigación, el delito presuntamente cometido, la dirección de la moneda como el resultado de la solicitud pretendida que incluye historial de la transacción, usario, método de pago, mensajes, IP, etc.

Con el fin de evitar que estas plataformas se pudieran convertir en instrumento de fácil acceso dentro de la criminalidad organizada para el blanqueo de activos patrimoniales de naturaleza ilícita, la UE publicó la V Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015 que incorpora expresamente en materia de criptomonedas dos importantes novedades:

- En cuanto a su ámbito de aplicación, el *artículo 1* de la V Directiva[70] considera a los proveedores de servicios de monederos electrónicos como *sujetos obligados* a los efectos previstos en la Directiva 2015/849. Hay que recordar que tanto el conjunto de las denominadas Directivas anti-blanqueo como la transposición que de las mismas se llevó a cabo en nuestro ordenamiento jurídico de forma progresiva a

[68] La más utilizada a nivel policial en es BINANCE cuya filial española Moon Tech Spain obtuvo el registro como proveedor de servicio de activos virtuales por parte del Banco de España el 7 de julio de 2022. También existen otras como Kukoin o Crypto.com.

[70] El artículo 1 de la V Directiva modifica, entre otros, el artículo 1.c.g) y 1.c.h) de la Directiva 2015/849 incluyendo expresamente como sujetos obligados a los proveedores de servicios de activos virtuales.

través de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de financiación del terrorismo, impone a estos sujetos, con carácter general las siguientes obligaciones:

- Una diligencia debida a la hora de identificar y conocer a aquellas personas físicas o jurídicas que establezcan una relación comercial.
- Informar al SEBLAC lo que se consideren operaciones sospechosas.
- Llevar a cabo medidas de control interno, concretamente el establecimiento protocolos internos tendentes a evitar precisamente que estás actuaciones "sospechosas" faciliten de forma indiscriminada el blanqueo de capitales y/o la financiación del terrorismo.

- Se amplía la facultad de *las autoridades competentes,* a través de las entidades obligadas, para vigilar el uso de las monedas virtuales[71] y, de forma más precisa, a las Unidades de Inteligencia Financieras (UIF) nacionales para poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual[72].

Es evidente lo importante que es para la norma comunitaria, especialmente a fin de salvaguardar los intereses financieros de la UE, incidir en una adecuada regulación normativa de las *exchanges*. Sin embargo, debemos preguntarnos si realmente, transcurrido un cierto tiempo desde la publicación de la Directiva, se ha conseguido el propósito inicial de evitar la clandestinidad de estas operaciones. Al respecto, resulta como mínimo sorprendente que la Directiva admita en el Considerando 9 que la inclusión de los proveedores de servicios como sujetos obligados "*no resolverá la cuestión del anonimato asociado a las transacciones con monedas virtual*", focalizando el quid de la cuestión en que actualmente ese anonimato, tapadera de muchas organizaciones delictivas, sigue estando latente en el entorno de las criptomonedas.

[71] Vid Considerando 8 de la V Directiva.
[72] Vid Considerando 9 de la V Directiva.

Finalmente hemos de reseñar que, en nuestro ordenamiento jurídico, la V Directiva ha sido objeto de trasposición a nuestro ordenamiento a través del Real Decreto-Ley 7/2021, de 27 de abril que introduce las siguientes novedades:

- Concreta lo que es un cambio de moneda virtual por moneda fiduciaria[73] y los que han ser considerados como proveedores de servicios de custodia de monederos electrónicos[74].
- Los proveedores de servicios que operen en España deberán fijar un representante ante el SEPBLAC,
- Se crea un "Registro Especial" donde deberán inscribirse los proveedores de servicios, asumiendo el Banco de España una función supervisora, tanto del cumplimiento de inscripción como de sanción en caso de incumplimiento.

A la vista de lo expuesto podemos concluir que las reformas legislativas acometidas en el seno de la UE, aun siendo necesarias, dejan sin resolver el gran problema que planea en la regulación de los proveedores de servicios, y que no es otro que la ausencia de un debido control de verificación sobre la persona que se encuentra detrás de aquella que físicamente formaliza la creación de la billetera electrónica. Como es lógico, estos sujetos se encuentran "contratados" por organizaciones criminales que los utilizan a modo de pantalla, dificultando la obtención del titular real, que no ficticio de la *wallet*. Se detecta además un problema adicional, pues mucho de estos proveedores ofrecen sus servicios fuera del territorio nacional, lo que dificulta, por no decir, imposibilitan la investigación ante la ausencia de unos mecanismos rápidos y eficaces de cooperación penal internacional.

[73] Así el art.1, apartado 6 considera un cambio de moneda virtual por moneda fiduciaria "*como 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.*

[74] El art. 1, apartado 7 define a los proveedores de servicio de custodia de monederos electrónicos a "*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."*

- La averiguación de la clave privada.

Sin duda alguna el gran desafío que se les plantean a las unidades especializadas de fiscalía o al juez de instrucción, una vez obtenida la dirección pública, es cómo acceder a una clave que se encuentra encriptada y cuyo conocimiento "a priori" tan sólo conoce su titular. En este sentido, las alternativas no son muchas, lo que no impide que debamos analizarlas desde una perspectiva operativa:

- Antes del denominado "día de acción"[75], se han de acudir a la utilización de medidas limitativas de derechos fundamentales, siempre bajo el secreto de las actuaciones, destacando las siguientes:

    i. La colocación de vídeos y cámaras en el interior de una estancia donde se pueda estar utilizando un ordenador, teléfono o dispositivo[76]. Aquí la dificultad estriba en la adecuada colocación del dispositivo de vigilancia, debiéndose ponderar el momento de su instalación para no ser detectado por el sujeto y en una zona que permita "visualizar" correctamente como se hace uso de la clave.
    ii. Empleo de agentes encubiertos informáticos[77]. Se trata de un instrumento de investigación altamente valioso para el proceso penal pero que, por el contrario, requiere un alto conocimiento técnico que dificulta en muchas ocasiones su utilización como forma de infiltración en la delincuencia organizada.
    iii. Acceso en la red informática mediante *phishing*, bastando el envío de un link al correo o terminal del investigado. Sin embargo, el alto grado de especialización técnica de los potenciales destinatarios hace que sea poco útil esta medida en la práctica.
    iv. Registro remoto sobre equipos informáticos[78]. Aquí la problemática resida en lo costoso que supone el empleo de un

[75] En la jerga policial se conoce como el día señalado para realizar todas las operaciones contra los investigados, tales como detenciones, entradas y registros e incautación de bienes
[76] Vid art.588 quarter de la LECrim.
[77] Vid art. 282 bis de la LECrim.
[78] Vid art.588 septies de la LECrim.

software adecuado que permita monitorizar los movimientos que realiza el investigado en su terminal, ya sea ordenador, tablet o móvil así como la complejidad técnica que supone la ejecución material de la medida.

- Tras "el día de acción", lo lógico es que se produzcan, entre otras diligencias, la entrada y registro en los domicilios de los investigados, en cuyo interior pudiera encontrarse materialmente la clave anotada en un monedero de papel o en el volcado de algún soporte informático. Es obvio que esos casos son poco probables dadas las enormes medidas de prevención utilizada, todas ellas dirigidas a evitar que se conozca la clave. Otra alternativa es contar con la colaboración del investigado, eso sí, debiéndose respetar y sobre todo informar de forma escrupulosa de sus derechos constitucionales reconocidos en los artículos 118 y 520 de la LECrim, especialmente si ha sido objeto de detención policial.

De un breve análisis de lo expuesto hasta el momento, se puede constatar que, desde un punto de vista práctico, la ausencia de un marco legal en la materia con unas directrices básicas y estandarizadas, convierte la averiguación de la dirección pública y de la clave privada en una auténtica odisea para las unidades de investigación policial, resultando esencial, como hemos advertido, el uso eficaz de las medidas de investigación tecnológicas, las cuales, algunas veces no son del todo suficientes para la obtención de la clave.

2.2. La adopción de medidas cautelares

Una vez se accede virtualmente al interior de la *wallet*, se puede conseguir mucha información sobre el resultado de las transacciones realizadas. De hecho, el éxito final de la investigación radica no sólo en poder incautar las criptomonedas, sino en obtener aquellos elementos de prueba que vinculen al investigado con las actividades económicas ilícitas realizadas. Se ha de tener presente, además, que la cantidad final de criptomonedas que una persona tenga asociada una determinada dirección pública es resultado del número de transacciones realizadas, de ahí la importancia de conocer esta información.

Ahora bien, ¿qué tipo de medidas cautelares son factibles para evitar que desaparezcan del interior de la billetera las criptomonedas? No es ésta

una cuestión baladí, pues una de las características de la tecnología DLT es la enorme volatilidad de las operaciones efectuadas. Sin embargo, no basta una mera resolución judicial en la que se acuerde el bloqueo o intervención de las criptomonedas ni tampoco existe un protocolo de actuación policial que determine qué hacer en este tipo de casos. De nuevo, la práctica forense ofrece las siguientes alternativas en función del momento en que sean adoptadas las medidas y de las características de la *wallet* intervenida:

2.2.1. Medidas de aseguramiento inmediato realizadas por la Policía Judicial

En primer lugar, si la criptomoneda se encuentra en una "billetera caliente", se ha de "cortar" de inmediato la conexión a Internet del monedero ya que de lo contario se corre el riesgo de que terceras personas puedan tener acceso a la clave o puedan hackearla a través de equipos remotos.

En segundo lugar, si las criptomonedas se encuentran en una "cartera fría", en un monedero de papel o ya efectuada la desconexión de la red, lo correcto es crear un monedero gemelo o "a la par" preferentemente en formato papel. La finalidad perseguida no es otra que la obtención de un nueva *wallet* con las operaciones realizadas de la billetera intervenida y a disposición de la autoridad judicial, lo que requiere, por un lado, la copia de la clave privada o importación y, lo más importante, arrastrar toda la información del anterior monedero al nuevo necesitando, como es lógico, conexión a la red.

Una vez más se plantea un problema de naturaleza logística, aunque con claras consecuencias penales ¿qué hacer con la nueva billetera generada "ad hoc" por la unidad policía investigadora? Sin duda alguna la custodia policial ha de dar paso, como veremos a continuación, al exhaustivo control judicial de las misma.

2.2.2. Medidas de intervención judicial

A nuestro parecer, la responsabilidad en la custodia de la *wallet* intervenida policialmente ha de recaer en el Letrado de la Administración de Justicia con la supervisión del Juez de Instrucción. Efectivamente, y con independencia de la naturaleza jurídica que se pretenda dar a las

criptomonedas, no deja de ser un efecto judicial al amparo del artículo 368 bis de la LECrim, que incluso puede operar como medio de prueba en el proceso. Por lo tanto, una vez puesto a disposición de forma material el monedero en "papel" se ha de adoptar una resolución judicial debidamente motivada en la que se acuerde el embargo preventivo de la criptomoneda y se expliquen los motivos por los que se acuerda, ya sea para garantizar el decomiso final si es un producto ilícito, ya sea para asegurar un elemento de prueba o si es para satisfacer algún tipo de responsabilidad civil.

Ahora bien, no basta con la adopción de la medida, sino que dicha resolución ha de concretar la forma en que se va a llevar a cabo el control de la clave privada y de la información que contiene la *wallet* creada en su interior. Aquí, de nuevo, surgen las siguientes posibilidades:

- Que la criptomoneda se encuentra custodiada en todo momento por el órgano jurisdiccional. En este caso lo procesalmente correcto, aunque no esté previsto en la LECrim, es la formación de una pieza separada que incluya la *wallet* generada con el "barrido" de la información obtenida y la clave privada importada. El riesgo evidente, dada la frecuencia con la que se produce, es que se pueda extraviar la pieza separada, resultando aconsejable que a través del LAJ sea depositada en una caja de seguridad en una entidad bancaria habilitada del Juzgado.
- Que se acuerde la "encomienda" en la gestión del depósito a la ORGA. La naturaleza jurídica de este organismo creado por la Orden JUS/188/15, de 23 de octubre es, quizás, la opción más segura al disponer de medios suficientes "para evitar actuaciones antieconómicas, obtener el beneficio económico, dentro de la ley y con todas las garantías procesales."[79]

- Que se proceda a la enajenación anticipada de la criptomoneda de conformidad con el artículo 367 septies de la LECrim, convirtiendo la moneda virtual en dinero fiduciario, debiéndose igualmente formar pieza separada y dando trámite a las partes.

[79] Art. 2 de la Orden JUS/188/2016, de 18 de febrero, por la que se determina el ámbito de actuación y la entrada en funcionamiento operativo de la Oficina de Recuperación y Gestión de Activos y la apertura de su cuenta de depósitos y consignaciones

De las tres alternativas expuestas, consideramos que la que más garantías ofrece es la "delegación" por el Juez de Instrucción de la *wallet* a la ORGA, no sólo por disponer de mejores medios, sino por que, precisamente por su carácter especializado, pretende, entre otros objetivos, la conservación de cualquier tipo de activo patrimonial intervenido judicialmente. Por otra parte, la ventaja que ofrece la venta anticipada, al margen de la obtención de dinero efectivo, que facilita su disponibilidad inmediata en la causa penal, es la de evitar el problema de la constante fluctuación de la moneda virtual, con el consiguiente problema que supone determinar el valor real de la criptomoneda intervenida, especialmente si ha transcurrido un largo tiempo desde el momento de su intervención y hasta que finalmente es decomisada o restituida al perjudicado.

3. DECOMISO

La figura del decomiso es definida en el artículo 2 de la Directiva 2014/42/UE de 3 de abril[80], como "*la privación definitiva de un bien por un órgano jurisdiccional en relación con una infracción penal*". Dejando al margen su discutida naturaleza jurídica, lo que no se puede poner en duda es la enorme relevancia adquirida por este instrumento en la lucha contra la delincuencia organizada. Sin embargo, ni la Directiva 2014/42 ni el Reglamento 2018/1805, de 14 de noviembre, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso ofrecen un tratamiento diferenciado o, al menos, mínimamente destallado de lo que es decomisar un criptoactivo. Tampoco resulta muy esperanzadora la Propuesta de Directiva sobre recuperación y decomiso de activos de 25 de mayo de 2022[81] , en cuyo Considerando 12 de forma tangencial incluye a los criptoactivos "como cualquier forma de bien" que permita transformar y ocultar efectos relacionados con el delito.

El decomiso, por lo tanto, sigue siendo hoy la gran asignatura pendiente en el proceso penal, a pesar de las continuas reformas operadas

[80] Directiva 2014/42/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014 sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea**.**

[81] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre recuperación y decomiso de activos Bruselas, 25.5.2022 COM(2022) 245 final

en nuestro ordenamiento consecuencia de la transposición de la citada Directiva 2014/42/UE. Por lo tanto, teniendo presente el ámbito de aplicación de la actual normativa comunitaria, se podrían dar, a nuestro juicio, los dos siguientes posibles escenarios:

- La criptomoneda como *producto* del delito, es decir, que haya servido para la obtención de un beneficio ilícito o una ventaja económica derivada de la infracción penal. Lo que se pretende en estos casos es el estrangulamiento financiero de la organización, evitando la acumulación de activos patrimoniales que pudieran revertir negativamente en la economía de los Estados miembros.

- La criptomoneda como *instrumento* del delito. Aquí la criptomoneda es utilizada para favorecer o, simplemente, cometer el delito, lo cual, la convierte "ipso facto" en un elemento de prueba a ser valorado en el juicio oral. Es cierto que en algunas ocasiones es difícil trazar la línea que separa lo que ha sido consecuencia y lo que ha servido para la comisión del delito. No se trata de una cuestión baladí, pues en el primero de los casos habrá de acudirse a los instrumentos que regulan el embargo y el decomiso, mientras que, en el segundo supuesto, se utilizará la OEI como forma de cooperación, ya sea para averiguar el origen de las criptomonedas o, en su caso, como manera de asegurarla como elemento de prueba.

4. LA RESTITUCIÓN DE LA CRIPTOMONEDA: INDEMNIZACIÓN A LA VÍCTIMA

Se trata esta de una cuestión sumamente interesante, aunque resuelta, en cierto modo, por la STS 325/2019 de 20 de junio. Efectivamente, en el caso de que no se haya producido una realización anticipada en sede instructora, lo que se plantea es determinar qué es lo que ha de entregarse al perjudicado, si la criptomoneda sustraída ilegítimamente en el momento en que se cometió el delito con su valor actual[82] o, por el contrario, el

[82] La Sala de lo Penal del Tribunal Supremo (TS) resuelve un recurso de casación por un delito continuado de estafa. Concretamente lo que lo que se discutía era la creación de una empresa de compra y venta automatizadas en segundos de bitcoins, realizándose diversas inversiones varios perjudicados sin obtener una contraprestación a cambio. La

importe de la aportación dineraria realizada en su momento por la víctima. Efectivamente una de las características especialmente de los bitcoins es su fluctuación que hace imprevisible, a diferencia de activos financieros seguros, el valor que puede tener a corto o medio plazo.

Aunque no es el momento de realizar un análisis exhaustivo de la cuestión, lo más relevante de la citada sentencia del TS es que se aparta de la doctrina de la restitución del bien objeto del delito conforme a los artículos 110 y 111 del Código Penal y, tras ratificar la decisión acordada por el tribunal de instancia considera más apropiado conforme a la naturaleza del bitcoin, entender que se ha producido un daño al perjudicado, de ahí que proceda su reparación con un incremento que equipara al "*perjuicio derivado de la rentabilidad que hubiera ofrecido el precio de las unidad de bitcoins entre el momento de la inversión y la fecha de vencimiento de sus respectivos contratos*."[83]. Por lo tanto, la criptomoneda no se *restituye* tal cual, como pudiera ser cualquier objeto intervenido judicialmente en la causa penal, sino un valor equivalente al daño producido-se entiende por la inversión inicial-y el perjuicio económico ocasionado-por las ganancias dejadas de obtener-.

A nuestro juicio se trata de una decisión correcta. De haberse optado por la primera vía, se correría el grave riesgo de que el valor final de la criptomoneda dependa del momento en que se publicara la decisión judicial que acordara la indemnización al perjudicado. Es cierto que, para llegar a dicha conclusión, se entiende que el bitcoin no se puede devolver "*al no ser dinero ni un bien tangible*", lo cual es ciertamente discutible desde el mismo momento en que es considerado un activo patrimonial y, por ende, equiparable a otros valores financieros altamente volátiles. Habrá que esperar a otros pronunciamientos que no se ciñan exclusivamente al bitcoin o no tengan causa directa en una estafa a la víctima, como pudiera ser, a modo de ejemplo, un hackeo en el móvil de una persona con sustracción de moneda virtual, o en pagos autorizados y no devueltos.

CONCLUSIONES Y RETOS ACTUALES

Audiencia Provincial de Madrid ordenó restituir el valor de cotización de esta moneda virtual al momento de finalización de los respectivos contratos

[83] Fundamento jurídico 3º.

El régimen jurídico de las criptomonedas en general y de los bitcoins en particular, representa un reto sin precedente dentro del Espacio Judicial Europeo. La actual regulación legislativa se encuentra totalmente alejada del vertiginoso avance de las TICs, lo cual no sólo facilita la actividad criminal a gran escala, sino que ha encontrado una vía para que cualquier persona con ciertos conocimientos informáticos pueda verse beneficio del ciberespacio para la comisión impune de delitos. A la espera del impacto normativo en la UE que pueda tener el Reglamento MICA, los índices de cibercriminalidad, especialmente puestos de manifiesto por los informes de Europol, alertan del grave riesgo que supone para los intereses financieros de los Estados el uso abusivo e incontrolado de las criptodivisas.

Para paliar a nivel institucional este problema resulta necesario, como mínimo, fijar una hoja de ruta que, a nuestro juicio, pasaría por desarrollar e implementar los siguientes aspectos:

1.º- Garantizar la confianza en la adquisición de criptoactivos, lo cual sólo es posible con un planteamiento común en la UE que permita saber con suficiente antelación, no sólo lo que es una criptomoneda, sino los componentes jurídicos que conlleva su ámbito de aplicación. El enorme potencial que representa la inversión de la moneda virtual no puede convertirse en una vía de escape rápida para la proliferación de actividades ilícita, especialmente, aquellas cuyo último fin es el blanqueo de dinero, aunque también vinculadas a delitos de naturaleza patrimonial, como estafas o ataques cibernéticos a empresas a cambio de un determinado rescate.

2º.- Fortalecer el sistema normativo actual, con unos parámetros comunes entre los Estados miembros que permitan adecuar sus legislaciones a la realidad actual de las criptomonedas. A la espera de lo que pueda suponer el Reglamento MICA, una de las propuestas que, a nuestro modo de ver las cosas, evitaría la proliferación delictiva vinculada a la moneda virtual, sería su obligatoria conversión a moneda *fiat* transcurrido un breve tiempo, favoreciendo una mayor transparencia, especialmente a nivel tributario, tanto en la tenencia como en la ulterior transferencia de criptoactivos. En este sentido resulta esencial que la consideración de los proveedores de servicios o *enchangers* como sujetos obligados no se convierta en papel mojado e identifiquen adecuadamente

operaciones sospechosas o que, una vez requeridos, aporten de forma inmediata la mayor información posible de una billetera.

3º.- Vincular su regulación a la actual política criminal de que el delito no resulte beneficioso. Sólo desde una política de prevención basada en una adecuada y eficaz lucha en la recuperación de activos financieros, en lo que hay que incluir las criptomonedas, es posible el estrangulamiento financiero de estas organizaciones criminales favorecidas, hasta el momento, por un escenario un tanto difuso.

4º.- Mejorar los mecanismos de cooperación penal internacional, especialmente a la hora de la obtención de información estratégica vinculada a la ciberdelincuencia, lo cual pasaría por agilizar las vías de comunicación a nivel policial y determinar claramente qué jurisdicción es la competente en caso de el cibercrimen se cometa en varios Estados. Igualmente se deberían implementar un procedimiento de gestión estandarizado en el que las oficinas AROs asuman el control a la hora de almacenar los monederos virtuales, evitando cualquier tipo de intromisión ilícita.

BIBLIOGRAFÍA

Aránguez Sanchez, Carlos (2020), "El Bitcoin como instrumento y objeto del delito*", en Cuadernos de Política Criminal*, Madrid, Dykinson.

Arias Merlano, Jonahna Carolina (2019), "El creciente uso de las criptomonedas para la comisión delictiva*", en Unión Europea, incidencia en la economía y sociedad digital, aplicación de las reformas recientes e internacionalización del derecho penal*, Madrid, Tirant lo Blanch, pp 487-492.

Capriglia, Aceto di (2020), "Monedas virtuales y cibercrímenes. Un análisis comparativo", en *Revista Boliviana de Derecho*, La Paz, Tirant lo Blanch.

Cavada Herrera, Juan Pablo (2020), Cibercrimen y delito informático. Definiciones en legislación internacional, nacional y extranjera, Chile, Biblioteca del Congreso Nacional de Chile.

Fernández Morlanes, Rafael (2018), "Las criptomonedas y el bitcoin como fenómeno disruptivo: proyección jurídica en el ámbito penal*", en Cuadernos Digitales de Formación,* Madrid, CGPJ.

Fernández Morlanes, Rafael (2018), "Las criptomonedas y el bitcoin como fenómeno disruptivo: proyección jurídica en el ámbito penal*", en Cuadernos Digitales de Formación,* Madrid, CGPJ.

Padilla Ruiz, Pedro (2019), "Los bitcoins no se restituyen a la víctima de estafa al no ser dinero. Giro radical de la doctrina del Tribunal Supremo*", en Revista Aranzadi Doctrinal.* Madrid, Aranzadi.

Pérez López, Xesús (2017), "Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y España", en *Revista de Derecho Penal y Criminonología*, Madrid, UNED.

Jiménez-Villarejo Fernández, Francisco (2020), "Recuperación de activos en la Unión Europea" en *Decomiso y Recuperación de Activos. Crime doesn´t pay*, Madrid, Tirant lo Blanch, pp 295-398.

Navarro Cardoso, Fernando (2019): "Criptomonedas (en especial, bitcoin) y blanqueo de dinero" en *Revista Electrónica de Ciencia Penal y Criminología*, Madrid, núm. 21-14, pp 31-33

Pérez Medina, Devika (2020), "Blockchain, criptomonedas y los fenómenos delicitivos: entre el crimen y el desarrollo" en *Boletín Criminológico,* Málaga, Instituto Andaluz interuniversitario de Criminología.

Quesada López, Pedro Manuel (2021), "Breves notas sobre la investigación de delitos en los que intervengan criptomoneda", en *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos,* Madrid, Thomson Reuters.

Rodríguez Juanico, Pablo (2020), "Breves notas sobre la investigación de delitos en los que intervengan criptomonedas", en *Diario la Ley,* Madrid. Wolters Kluwer.

Rodríguez Medel, Carmen (2020), "España como país emisor de decisiones de embargo y decomiso en el Reglamento (UE) 2018/1805 en *Decomiso y Recuperación de Activos. Crime doesn´t pay, Madrid,* Tirant lo Blanch, pp 425-448.

Ruano Mochales, Teresa (2020), "Monedas virtuales y la normativa sobre blanqueo de capitales y la financiación de terrorismo" en *Diario la Ley,* Madrid. Wolters Kluwer.

Tapia Hermida, Alberto J. (2022), "Desafíos en la regulación y supervisión de los criptoactivos en la Unión Europea y en España" en *La Ley,* Madrid. Wolters Kluwer.

Velasco Nuñez, Eloy (2020), "Aspectos jurídicos penales vinculados al blockchain y las criptomonedas: delitos fiscales, blanqueo de capitales, robo, estafa", en *Cuadernos Digitales de Formación,* Madrid, Sepin.