Las criptomonedas frente al delito de blanqueo de capitales y la complejidad de la prueba pericial en el ámbito ciberdelincuente

ÁNGELA CASALS FERNÁNDEZ

Profesora Acreditada Contratada Doctora de Derecho Penal
y Derecho Penitenciario
Universidad CEU San Pablo
Doctoranda Universidad de Alcalá

RESUMEN

Hoy en día tenemos nuevos retos en el ámbito de la ciberdelincuencia, especialmente su regulación y complejidad en demostrar sus actuaciones ilegítimas. El presente trabajo se compone de un breve análisis de las criptomonedas y los usos ilegítimos de estas, con especial consideración del delito de blanqueo de capitales. Hay que tener en cuenta que la lucha contra el lavado de activos, entre otros constituye un reto crucial para los legisladores internacionales y nacionales, especialmente para desincentivar a los delincuentes de recurrir a las monedas virtuales para conseguir sus fines delictivos. La segunda parte del trabajo se dedica a la complejidad de la prueba pericial en el mundo cibernético, especial mención a la informática forense y al informe pericial informático.

Palabras clave: *Criptomonedas, delito de blanqueo de capitales, prueba pericial, ciberdelito, informe pericial.*

ABSTRACT

Today we face new challenges in the field of cybercrime, especially its regulation and complexity in proving its illegitimate actions. This paper consists of a brief analysis of cryptocurrencies and their illegitimate uses, with special consideration of the crime of money laundering. It should be borne in mind that the fight

against money laundering, among others, is a crucial challenge for international and national legislators, especially to discourage criminals from resorting to virtual currencies to achieve their criminal ends. The second part of the work is devoted to the complexity of expert evidence in the cyber world, with special mention of computer forensics and computer forensic reports.

Keywords: *Cryptocurrencies, money laundering, expert evidence, cybercrime, expert evidence.*

I. INTRODUCCIÓN

El ciberespacio lleva años consolidándose como un entorno de alta relevancia económica y social, pero también de inseguridad. Un ámbito propicio para la alta velocidad de cambio, donde los riesgos y amenazas son cambiantes, poliédricos, difíciles de evaluar y de predecir. Desde que en la década de los 90 aparecieran las tecnologías de la información y la comunicación, a través del surgimiento de la *World Wide Web*, se ha ido transformando el comportamiento humano a nivel mundial. El crecimiento imparable del uso de estas nuevas tecnologías ha favorecido la ampliación y la diversidad de los espacios y de las condiciones de comunicación social. En términos generales, podemos afirmar que hemos pasado a ser dependientes de las nuevas tecnologías y, al igual que nuestra forma de comunicación ha dado un salto evolutivo en estos últimos años este importante cambio también se ve reflejado en nuevas formas de cometer delitos(1).

La realidad virtual configurada por las nuevas tecnologías es un espacio no tangible que guarda muchas similitudes con los espacios físicos propios de la realidad material, por lo que debe recibir la misma

(1) Vid. Cerezo Domínguez, A. I. «La ciberdelincuencia en España: un estudio basado en las estadísticas policiales», en *Revista de Estudios Penales y de la Seguridad* núm. 6, 2020, p. 3.

protección jurídica que estos. El vigente Código Penal tiene un número considerable de nuevos artículos referentes al mundo tecnológico. Las exigencias del principio de legalidad han obligado a nuestro legislador a incorporar, en todos los delitos en los que existe una relación de instrumentos comisivos, una referencia expresa a los medios tecnológicos y en algunos casos diseñar nuevas infracciones cuya acción típica consiste, exclusivamente, en la utilización de nuevas tecnologías(2).

Debemos recordar que para que proceda la punición de un daño un bien jurídico protegido, realizado a través de medios o instrumentos informáticos, electrónicos o cibernéticos, no es inexcusable que el Código Penal recoja una mención expresa. Nos encontramos que, a veces, el legislador ha optado por describir la conducta típica del delito con una expresión genérica, abarcando todos los medios e instrumentos capaces de provocar el resultado no permitido. Por ejemplo, en el artículo 169 del Código Penal donde expresa «se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción»; o en el artículo 172 ter del Código Penal que dice que se puede dar acoso «a través de cualquier medio de comunicación».

Además, debemos tener en cuenta que hay dos grandes retos, entre otros, en la ciberdelincuencia. Por un lado, el conflicto jurisdiccional, ya que el tratamiento de los datos informatizados es un factor criminológico con una facilidad en su acceso, obtención y uso, traduciéndose en una dificultad para la determinación del autor y los medos de prueba. Esto se debe a que es una red de comunicación global sujeta de forma simultánea a varias jurisdicciones limitadas por el factor territorial frente a la multiterritorialidad que caracteriza a la red y que a efectos de la persecución de la ciberdelincuencia se traduce en una plurijurisdiccionalidad(3). Internet ha sido capaz de desarrollar un sistema de comunicación y transmisión de datos de carácter universal(4)

---

(2) Como, por ejemplo, el artículo 197 bis.2 del Código Penal que pena la utilización de artificios o instrumentos técnicos para interceptar transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información; o el artículo 270.2 del Código Penal donde la conducta es la facilitación de modo activo el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios. En Mestre Delgado, E.: «Introducción», en VV. AA.: *Tratado de Delincuencia Cibernética,* Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 58.

(3) Vid. Muñoz Machado, S.: *La regulación de la red. Poder y Derecho en Internet,* Taurus, Madrid, 2000, p. 221.

(4) Vid. Morales García, O.: «Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información», en *Cuadernos de Derecho Judicial* núm. 9, 2002, p. 237.

frente a la incapacidad político-gubernativa de optar, o por el establecimiento de una homogeneización o una legislación internacional, para unificar las tipologías previstas en el derecho penal sustantivo(5).

Por otro lado, la gran problemática con el aspecto probatorio y la acreditación de la conducta para poder identificar la autoría. Ejemplo de ello, y adentrándonos en nuestro tipo delictivo objeto de estudio, donde a través de grandes operaciones en red se comete delito de blanqueo de capitales teniendo las evidencias digitales las pruebas de los ilícitos que se han cometido. De ahí la importancia de analizar documentos informáticos, correos electrónicos, mensajes en el móvil o incluso la geolocalización para poder determinar en qué lugares ha estado el investigado. De ahí la importancia de tener que acudir a la prueba pericial informática o de carácter tecnológico para poder acreditar el hecho delictivo y la autoría, sirviendo ésta al Juez para poder formarse su convicción(6).

Adentrándonos en nuestro complejo tema de estudio, el uso de las criptomonedas presenta grandes dificultades por el carácter descentralizado, la difícil trazabilidad de sus movimientos por su grado de privacidad y su habitual irreversibilidad de las transacciones(7), de ahí que sean presupuestos con una orientación hacia usos ilegítimos.

II. REPRESENTACIÓN DIGITAL DE VALOR: LAS CRIPTOMONEDAS

Las criptomonedas carecen de una regulación jurídica unitaria y esta circunstancia caracteriza la relevancia penal de los comportamientos que se comenten mediante las mismas. Su régimen jurídico penal, al igual que su régimen jurídico en general, resulta discontinuo y fragmentario, lo que complica la descripción de los riesgos penales derivados de la creación y funcionamiento de las criptomonedas(8).

(5) Vid. Velasco Núñez, E.: «Ciberseguridad, ciberdelincuencia y empresa: la respuesta penal», en *Revista de privacidad y derecho digital*, vol. 4, núm. 14 (abril-junio), 2019, p. 25.

(6) Vid. Martínez Galindo, G.: «La prueba pericial informática y tecnológica», en VV. AA.: *Tratado de Delincuencia Cibernética*, Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 741.

(7) Vid. Pérez López, X: «El blanqueo de capitales a través de las criptomonedas», en VV. AA.: *Tratado de Delincuencia Cibernética*, Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 511.

(8) Vid. Barroilhet Díez, A.: «Criptomonedas, economía y derecho», en *Revista chilena de derecho y tecnología,* vol. 8, núm. 1, 2019, p. 31.

A esta tarea hay que añadir además otra dificultad, la variedad de monedas virtuales que tienen cabida dentro de este concepto, con diversas características y grados de control por parte de sus operadores y la rapidez con la que aparecen otras nuevas. En la actualidad, existen más de 10.400 criptomonedas(9).

La primera controversia que surge acerca de la criptomoneda es su calificación como dinero, moneda o divisa. En 2008, a través de un escrito realizado por Satoshi Nakamoto(10), se proponía la denominación de *bitcoin*, describiendo un sistema propuesto como *peer-to-peer* de dinero en efectivo electrónico, siendo un sistema de pagos que, por no requerir de un tercero cuya autoridad respaldase la validez de la transacción para la fiabilidad de ésta, constituiría una alterativa viable al dinero contante en las transacciones online(11).

La Unión Europea ha dado ya los primeros pasos en la regulación del mercado de los criptoactivos y en abril de 2020 la Comisión presentaba una propuesta de regulación, a través de la Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM (2020) 593 final, 2020/0265 (COD).

En 2018 se desarrolla la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo, que tiene como finalidad considerar sujetos obligados a las personas que realizan dos actividades claves en el comercio de criptomonedas, por un lado, los proveedores de servicios de cambio entre las monedas virtuales y las fiduciarias, y, por otro lado, los proveedores de servicios de monedero. Además, la Directiva define la moneda virtual como «representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medos electrónicos».

En 2019, el Tribunal Supremo, en su STS 2109/2019, de 20 de junio, declara que las criptomonedas no son dinero de curso legal, sostiene que se trata de un activo patrimonial inmaterial de contraprestación o intercambio en aquellas transacciones bilaterales en las que los

(9) Según *CoinMarketCap* (coinmarketcap.com), es una plataforma online que realiza un seguimiento de la capitalización de diferentes criptomonedas, la cantidad de operaciones que las utilizan y el precio actual convertido a moneda fiduciaria.

(10) Se considera de Satoshi Nakamoto puede ser el pseudónimo usado por un grupo de personas, creadoras del protocolo *Bitcoin* y su *software* de referencia. NAKAMOTO, S.: «Bitcoin: A Peer-to-Peer Electronic Cash System», en *bitcoin.org*. Disponible en: https://bitcoin.org/bitcoin.pdf

(11) Cfr. PÉREZ LÓPEZ, X: *op. cit.*, p. 513.

contratantes lo acepten. El Banco Central Europeo(12) ha adoptado también esta postura, indicando que las monedas virtuales no son dinero ni monedas desde una perspectiva legal. Menos clara, sin embargo, resulta la posición del TJUE; se ha referido al bitcoin como 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 (STJUE 718/2015, de 22 de octubre).

Por lo tanto, y según la Directiva 2014/62/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la protección penal del euro y otras monedas frente a la falsificación, se entiende moneda de curso legal aquellas que tienen que ser obligatoriamente admitidas como medios de pago. Además, a día de hoy, las criptomonedas se encuentran fuera del ámbito de la legislación de la Unión Europea en materia de servicios financieros y no se encuentran sujetas a las disposiciones relativas a la protección de los inversores y la integridad de los mercados.

Aunque jurídicamente las criptomonedas no sean dinero, ni activos financieros, sí se pueden considerar bienes de consumo(13), ya que puede utilizarse como medio de pago y en el que algunos ciudadanos deciden invertir sus ahorros. Al ser un bien de consumo le es aplicable el derecho que tutela a los consumidores, incluida la publicidad engañosa que se encuentra en la Directiva 2006/144/CE del Parlamento Europeo y del Consejo, de 12 de diciembre, sobre publicidad engañosa y publicidad comparativa.

Además de considerarlas bienes de consumo, son un medio de pago. La Directiva 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, ha incluido a las criptomonedas dentro de las monedas virtuales, a las que define como «representación digital de valor que no ha sido emitida ni está garantizada por un banco central ni por una autoridad pública, no está necesariamente asociada a una moneda de curso legal ni posee la condición jurídica de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y nego-

(12) Vid. Banco Central Europeo: «Virtual currency schemes: A further análisis», Frankfurt am Main, 2015. Disponible en: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

(13) Cfr. Nieto Martín, A., García-Moreno, B.: «Criptomonedas y derecho penal: más allá del blanqueo de capitales», en *Revista Electrónica de Ciencia Penal y Criminología,* 23-17, 2021, p. 4. Disponible en: http://criminet.ugr.es/recpc/23/recpc23-17.pdf

ciarse por medios electrónicos». Y es que, son una clase de monedas virtuales que se caracterizan por utilizar para su circulación, una determinada tecnología, un registro de transacciones descentralizado, pero unitario, que utiliza la criptografía como mecanismo de seguridad. Esta tecnología es lo que conocemos como *blockchain* y, en lo que a nosotros nos interesa, confiere un gran protagonismo a la criminalidad informática como herramienta para realizar las diversas conductas delictivas en este entorno.

En España, nuestra norma de transposición no llega hasta la promulgación del Real Decreto-Ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores. Nuestro interés se centra en las novedades en materia de prevención del blanqueo de capitales, el artículo 3.1 que modifica la Ley 10/2010, realiza el cambio de moneda virtual por moneda fiduciaria; y se añaden las definiciones de proveedores de servicios de custodia de monederos electrónica y de moneda virtual.

Debemos destacar que nuestro legislador busca deslindar el nuevo concepto legal de moneda virtual con respecto a otros conceptos legales ya existentes, de índole monetaria(14). En la propia definición no sólo evita el calificar moneda virtual como dinero en general, sino que, además, trata de delimitar los contornos de la moneda virtual respecto a los de la moneda de curso legal y el dinero electrónico.

Hay que tener en cuenta que el blanqueo de capitales y la financiación del terrorismo son dos de los usos ilegítimos más conocidos de la regulación jurídico penal de las criptomonedas, toda vez que preocupa que puedan servir como medio de pago en transacciones ilícitas y como forma para introducir activos procedentes de actividades delictivas en la economía legal(15). El principal problema que tenemos en la actualidad para la economía y el sistema monetario es que las grandes masas de dinero procedentes de actividades delictivas ingresen en la economía legal. Es por eso por lo que las restricciones que el blanqueo de capitales impone sirven para el control del fraude fiscal. La Directiva 2018/843 del Parlamento Europeo y del Consejo somete a las monedas virtuales y las criptomonedas al mismo régimen que al dinero estatal, además se refiere a las posibilidades de uso

(14) Cfr. Pérez López, X: *op. cit*., p. 524.
(15) Vid. Nieto Martín, A., García-Moreno, B.: *op. cit*., p. 5.

de las criptomonedas en el contexto de la comisión de delitos de blanqueo de capitales.

Algunas de las principales características, según Pérez López(16), y tomando en consideración el *bitcoin*, para el empleo ilegítimo en el blanqueo de capitales son la comprobación y el registro de transacciones por la comunidad de usuarios, sin que sea posible la supervisión centralizada de éstas. En segundo lugar, la posibilidad de operar sin intermediarios. En tercer lugar, la dificultad para poder relacionar direcciones *bitcoin* de envío y de recepción de criptomonedas en las transacciones. En cuarto lugar, es imposible atribuir un identificador único a una unidad de valor, dificultando la trazabilidad de las transacciones. En quinto lugar, la dificultad para asociar un haz de direcciones *bitcoin* determinado a un usuario concreto. Y en sexto lugar la irreversibilidad de las transacciones una vez confirmadas.

Estas características en el mercado pueden considerarse ventajas dentro de las metodologías delictivas. Los informes institucionales(17) sobre la cibercriminalidad han destacado, en primer lugar, la ausencia de supervisión por parte de una autoridad central de índole estatal o bancaria. En segundo lugar, la posibilidad de llevar a cabo transacciones rápidas en un ámbito espacial que abarca todo el globo. Esto para el blanqueo de capitales no es un problema nuevo, las técnicas *offline* de movimientos de capitales con el fin de encubrir su origen ilícito pasaban y pasan por la fragmentación de la comisión del delito en una pluralidad de actos y de saltos de capitales de una jurisdicción a otra. Por eso la doctrina española ha resuelvo la fragmentación del *iter* delictivo del delito de blanqueo de capitales considerándolo un delito de resultado cortado y favoreciendo una concepción amplia de los bienes(18). Y, en tercer lugar, prácticamente el anonimato total, al tener una gran dificultad de relacionar a un usuario concreto con un haz de direcciones *bitcoin* determinado.

A día de hoy, podemos afirmar que las criptomonedas son un medio de pago frecuente en las finanzas criminales, siendo las más

(16) Vid. Pérez López, X.: «Las criptomonedas: consideraciones generales y empleo de las criptomonedas con fines de blanqueo», en Fernández Bermejo, D. (Dir.): *Blanqueo de capitales y TIC: Marco Jurídico y Europeo, Modus Operandi y Criptomonedas,* Thomson Reuters Aranzadi, Cizur Menor, 2019, p. 87.

(17) Entre otros, el Informe de 2014 del *Groupe de Travail «Monnaies virtuelles*» del *TracFin*; Informe anual del *Bundeskriminalam*t alemán de 2018; *Cybercrime- Bundeslagebild* de 2018.

(18) Vid. Fernández Bermejo, D. (Dir.): *Blanqueo de capitales y TIC: Marco Jurídico y Europeo, Modus Operandi y Criptomonedas,* Thomson Reuters Aranzadi, Cizur Menor, 2019, p. 33.

usadas de ellas en este contexto el *bitcoin*(19). Es frecuente el medio de pago en los *dark marketplaces*(20)*,* teniendo una gran cantidad de servicios que facilitan y ofrecen medios de cambio de criptomonedas por otro tipo de valores.

En 208, el Banco de España y la Comisión Nacional del Mercado de Valores emitieron una nota conjunta sobre los riesgos de la inversión en criptomonedas, poniéndolo en relación con las fuertes variaciones de la cotización de las principales criptomonedas en el inicio de 2017(21).

III. EL USO ILEGÍTIMO DE CRIPTOMONEDAS EN EL DELITO DE BLANQUEO DE CAPITALES

Desde los primeros años de existencia de las criptomonedas, se señaló como riesgos de la anonimidad con el dinero en efectivo, así como su carácter descentralizado. Esto último provocaba y provoca, dificultades para la investigación de los delitos de blanqueo de capitales, al no poder dirigirse las autoridades a una única entidad o administrador, además de la probabilidad de dispersarse geográficamente entre varias jurisdicciones las infraestructuras físicas que hacen posible el uso de las criptomonedas en cada caso determinado(22).

La utilización de criptomonedas como medio de blanqueo de capitales es, en la actualidad, una práctica de gran difusión entre los cibercriminales y que está también presente en el ámbito de la delincuencia no especializada en el medio *ciber*(23). Algunos *marketplaces* ofrecen a sus clientes el servicio de blanqueo de capitales o instrucciones acerca de cómo blanquear capitales empleando criptomonedas(24).

---

(19) Cfr. Europol, iOCTA (*internet Organised Crime Threat Assessment)* 2019, p. 54. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

(20) El listado de los *Darknet Markets* de 2022. Como, por ejemplo, *Alphabay Market, Vice City Market, Kingdom Market, DarkFox Market, Cocorico Market, Versus Marke*t. Disponible en: https://dnstats.net/list-of-darknet-markets/

(21) Banco De España; Comisión Nacional del Mercado de Valores: *Comunicado conjunto de la CNMV y del Banco de España sobre criptomonedas y ofertas iniciales de criptomonedas,* de 8 de febrero de 2018.

(22) Vid. Pérez López, X: «El blanqueo de capitales…», *op. cit.*, p. 541.

(23) Cfr. Europol, iOCTA (*internet Organised Crime Threat Assessment)* 2020, p. 58. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

(24) Ibíd., p. 59.

Debemos destacar, como así desarrolla Pérez López(25), que el empleo de criptomonedas como medio para el blanqueo de capitales no se suele presentar en solitario, sino que se acompaña de otros medios de naturaleza variada, siendo habitual la conversión sucesiva de los fondos a blanquear en distintos tipos de activos. Esto contribuye a una gran dificultad del seguimiento del rastro, obligando a las autoridades a combinar competencias técnicas muy específicas que requieren las investigaciones sobre criptomonedas con las competencias y acciones necesarias para el rastreo del producto delictivo hasta llegar al mundo físico.

Para poder llegar al mundo físico los propios criminales deben tener unas competencias específicas, necesitando recurrir a servicios específicos ofertados en los *dark marketplaces.* La metodología empleada en estos casos sigue un flujo circular. Se comienza por cambiar activos comprometidos, como las criptomonedas, a moneda de curso legal, desviándolas a una cuenta corriente concreta o a una multiplicidad de cuentas corrientes. De esas cuentas, los fondos son retirados en un cajero automático por miembros de la organización. Otras veces, a través de mercancías pedidas de manera fraudulente son recogidas por los miembros de la organización en negocios de paquetería o en apartados de correos. Una vez que cobran la comisión, los contratistas criminales devuelven los fondos restantes en criptomonedas a la organización criminal comitente, de este modo se cierra el círculo(26).

Adentrándonos en nuestra legislación y, en concreto, la conducta sancionada en el tipo básico del artículo 301.1 del Código Penal que dice que «el que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del estableci-

(25) Vid. Pérez López, X: op. cit., p. 543.

(26) Según el BKA, *Cybercrime- Bundeslagebild,* 2019, p. 40. Disponible en. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html; jsessionid=91C950CE5639A81ACEE2023BA455C7C3.live301?nn=28110.

miento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años». En este delito contra el patrimonio y el orden socioeconómico, es importante destacar la relación entre el delito previo y el blanqueo. Se consigue dar una apariencia de legalidad a un bien obtenido ilegalmente, permitiendo el uso y disfrute del mismo. Es lo que comúnmente se llama lavado de dinero y lo que pretende es borrar los rastros de la procedencia ilícita de una cantidad de dinero o un bien.

Teniendo en cuenta el entramado de operaciones que reviste el blanqueo, la jurisprudencia ha ido acotando paulatinamente una lista de indicios cuya concurrencia lleva a cabo la constitución de una prueba indiciaria sólida de la comisión de estos delitos. Esto lo refleja la STS 468/2018, de 7 de febrero, donde recapitula que constituyen los indicios más habituales de esta clase de infracciones, la inexistencia de justificación lícita de los ingresos que permiten la realización de esas operaciones; la naturaleza y características de las operaciones económicas llevadas a cabo, por ejemplo, con el uso de abundante dinero en metálico; la inexistencia de sociedades pantalla o entramados financieros que no se apoyan en actividades económicas acreditas de manera lícita. Este listado jurisprudencial de indicios habituales conecta con los usos ilegítimos actuales de las criptomonedas.

Revisando nuestra jurisprudencia, la SAN 14/2016, de 3 de marzo, versa sobre un complejo supuesto de cibercriminalidad con un gran alcance mediático, donde se da la estafa de pequeñas sumas de dinero a decenas de miles de personas en 22 países distintos entre los años 2011 y 2012 a través del uso de un *ramsomware*(27) de gran calidad técnica por una red criminal muy bien organizada. Dentro de los varios delitos por los que fueron condenados, se apreciaba la existencia de un delito de blanqueo de capitales con el uso de criptomonedas, no precisaba ninguna configuración de prueba indiciaria del delito, se limitaba a describir el entramado operativo empleado por la organización criminal. Se observó cómo se había procedido a realizar conversiones sucesivas del producto delictivo en diversos tipos de valores combinando diversos instrumentos financieros electrónicos y divisas de curso legal, el salto de los bienes de origen delictivo del formato digital al físico y viceversa con el fin de ofuscar su rastro, y la reserva final de los bienes blanqueados en instrumentos particularmente opacos, anónimos y de difícil investigación(28).

(27) El *ramsomwar*e es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Según https://es.malwarebytes.com/ransomware/

(28) Vid. Pérez López, X: *op. cit.*, p. 549.

La SAN 548/2021, de 7 de julio, en este caso, y en relación con los hechos «en fecha 10.2.2021 fue detenido en Alicante D. Cristóbal en virtud de orden de arresto emitida por el Tribunal Federal de Distrito para el Distrito Este de Kentucky de EEUU, con fines de extradición, para su persecución y enjuiciamiento por hechos delictivos que vienen calificados como delitos de estafa informática, organización criminal y blanqueo de capital. Incoado el procedimiento de extradición por el JCI, y puesta a su disposición el reclamado asistido de su letrado manifestó que no se acogía al procedimiento de extradición simplificada y que no renunciaba al principio de especialidad. Se decretó la prisión provisional por auto de 11.2.2021… Desde, por lo menos, diciembre de 2013 hasta diciembre de 2018, Cristóbal y otros integrantes de un grupo internacional de crimen organizado llevaron a cabo un ardid de fraude de subastas en línea que defraudó a residentes en Estados Unidos y ocasionaron pérdidas millonarias. Para llevar a cabo el ardid, Cristóbal y sus coconspiradores publicaron anuncios falsos en sitios web populares de subastas y ventas en línea por bienes costosos que no existían, crearon cuentas ficticias en línea para publicar los anuncios y se comunicaron con víctimas con el uso de identidades robadas y marcas registradas falsificadas. Después de recibir el dinero de las víctimas, Cristóbal y sus coconspiradores blanqueaban entonces esos fondos convirtiéndolos en criptomoneda y luego transferían la criptomoneda de vuelta a estafadores ubicados en el extranjero como Cristóbal, quien entonces se encargaba de transferir la criptomoneda a blanqueadores de dinero y cambiadores de criptomoneda ubicados en el extranjero. Los blanqueadores y cambiadores de dinero luego cambiaban la criptomoneda en moneda local para el beneficio de Cristóbal y sus coconspiradores».

Según nuestro Código Penal, los hechos constituyen un delito de estafa continuada de los artículo 248, 249, 250.5 y 74, un delito de blanqueo de capitales del artículo 301 y 302.1 y otro de pertenencia a organización criminal del artículo 570 bis.

Por último, y en cuanto al control por parte de España, debemos tener en cuenta la reforma del 28 de abril de 2021 que ha sufrido la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, en su nueva disposición adicional segunda exige la inscripción en un registro creado al efecto en el Banco de España de toda persona física o jurídica, sin que importe la nacionalidad, que preste u ofrezca en España servicios de cambio de moneda virtual por moneda fiduciaria o de custodia de monederos electrónicos; y la de toda persona física que preste estos servicios, cuando «la base, la dirección o la gestión de estas actividades radique en España», o toda

persona jurídica establecida en España que los preste, sin que importe dónde se ubiquen los destinatarios de tales servicios. Requiere la existencia de los procedimientos y los órganos adecuados para el cumplimiento de las obligaciones impuestas por la Ley 10/2010, así como los requisitos de honorabilidad comercial y profesional previstos en el Real Decreto 84/2015, de 13 de febrero, requisitos que se tendrán que mantener para continuar inscritos en el registro(29).

IV. LA PRUEBA PERICIAL EN EL ÁMBITO CIBERDELINCUENTE: LA INFORMÁTICA FORENSE

La prueba es el elemento determinante de los procesos judiciales en el ordenamiento jurídico español, de su práctica dependerá que el Juez obtenga la evidencia de los hechos controvertidos afirmados por las partes, que condicionan la aplicación de la norma cuya consecuencia jurídica las partes invocan(30). La prueba es, por tanto, la actividad procesal clave de la que depende que el juez logre su convencimiento acerca de los hechos litigiosos y, con base en las normas jurídicas aplicables, estime o desestime las pretensiones formuladas por las partes.

La prueba como entidad procesal adquiere una dimensión diferente con la expansión de las nuevas tecnologías. Las nuevas tecnologías no sólo han alterado las comunicaciones interpersonales, la obtención de la información por parte de los ciudadanos y su día a día, sino que han entrado de lleno en el derecho probatorio, pues han modificado las características propias de la prueba en los procesos judiciales(31).

La prueba pericial está prevista en el artículo 456 de la Ley de Enjuiciamiento Criminal que indica que «el Juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos». A su vez, la jurisprudencia (SSTS 2084/2001, de 13 de

(29) Desde la sede electrónica del Banco de España se informa del procedimiento para el registro, según

https://sedeelectronica.bde.es/sede/es/menu/tramites/autorizaciones-de-entidades-de-credito-y-otros/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html

(30) Vid. Gimeno Sendra, V.: l, *Derecho Procesal Civil I: El Proceso De Declaración. Parte General,* Ediciones Jurídicas Castillo de Luna, Madrid, 2015, p. 495.

(31) Vid. Arrabal Platero, P.: *La prueba tecnológica: aportación, práctica y valoración,* Tirant lo Blanch, Valencia, 2019, p. 32.

diciembre; 480/2009, de 22 de mayo; 1097/2011, de 25 de octubre) nos la define como una prueba de naturaleza personal que constituye una declaración de conocimiento de un especialista que aporta al Juez unos conocimientos técnicos.

Nos encontramos en la actualidad que tanto los delitos cometidos a través de las nuevas tecnologías, es decir, los ciberdelitos, como los delitos clásicos cometidos en el mundo *offline*, cuyas evidencias se encuentran en el ámbito digital o tecnológico, tienen una gran problemática en relación con el aspecto probatorio y la acreditación de la conducta para la identificación de la autoría, extracción de pruebas del delito y la posibilidad de desvirtuar el derecho a la presunción de inocencia(32).

En estos tipos de delitos cibernéticos es necesario acudir a la prueba pericial informática o de carácter tecnológico para poder acreditar el hecho delictivo y la autoría, para que el juez forme su convicción, siendo más o menos compleja en función del delito, por ejemplo, en nuestro caso el blanqueo de capitales con criptomonedas entraña una gran complejidad probatoria. Además, debemos tener en cuenta que en muchos casos se va a tratar del único medio de prueba o, incluso, la única basada en criterios objetivos, pudiendo aportar en el proceso una cierta convicción científica sobre la originalidad y autenticidad de una comunicación telemática o producida con las nuevas tecnologías(33).

Debemos recordar que en el ámbito de las pericias informáticas hay que citar a la informática forense, que es una disciplina dentro de la investigación en Ciencias Forenses. Su objeto es el estudio y análisis de sistemas informáticos para la obtención de pruebas y evidencias. Para todo ello, se requiere una continua actualización y esta disciplina desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales.

Las evidencias electrónicas son pruebas físicas de carácter inmaterial, normalmente rastros que quedan registrados en equipos o dispositivos informáticos o en el ciberespacio, siendo necesario ayudarse de esta ciencia para descubrirlos(34). Puede ser cualquier documento, fichero, registro o dato contenido en un soporte informático y que sea susceptible de tratamiento digital, como, por ejemplo, documentos de Ofimática, comunicaciones digitales, bases de dato, servidores, páginas web, entre otras.

---

(32) Vid. Martínez Galindo, G.: «La prueba pericial informática y tecnológica», en VV. AA.: *Tratado de Delincuencia Cibernética*, Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 741.

(33) Vid. Arrabal Platero, P.: *op. cit.*, p. 286.

(34) Cfr. Martínez Galindo, G.: *op. cit.*, p. 744.

Dentro de la informática forense encontramos disciplinas como el *Computer forensics,* que descubre e interpreta la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; el *Network forensics* que establece rastros, movimientos y acciones que un intruso ha desarrollado para concluir su acción en redes; y la *Digital forensics* que aplica los conceptos, estrategias y procedimientos de la moderna Criminalística a los medios informáticos(35). En la actualidad, la referencia para el análisis digital forense es la norma ISO/IEC 27037:2012, consiste en una guía para la identificación, recolección, adquisición y preservación de evidencia digital, procedente de Seguridad Informática ISO 27000, que es donde se proporcionan pautas para el manejo de la evidencia digital, sistematizando la identificación, recolección, adquisición y preservación de la misma, con procesos diseñados para respetar la integridad de la evidencia y con una metodología para asegurar su admisibilidad en el procedimiento judicial.

Los principios básicos en los que se basa la norma ISO/IEC 27037:2012 son los siguientes. En primer lugar, la aplicación de métodos. La evidencia digital debe ser adquirida del modo menos intrusivo posible, tratando de preservarla originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo. En segundo lugar, un proceso auditable. Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se deben proporcionar trazas y evidencias de lo realizado y sus resultados. En tercer lugar, un proceso reproducible. Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas. En cuarto lugar, un proceso defendible. Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación. Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias. En quinto lugar, una identificación. Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales información eso elementos de prueba en sus dos posibles estados, el físico y el

(35) Vid. Pinto Palacios, F., Pujol Capilla, P.: «La prueba pericial informática», en *Diario La Ley,* núm. 5, Sección Ciberderecho, 3 de abril de 2017, p.1. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMTEyMTS7Wy1KLizPw8WyMDQ3MDEwNjkEBmWqVLfnJIZUGqbVpiTnEqAJMEE-w1AAAAWKE

lógico, según sea el caso de cada evidencia. En sexto lugar, una recolección y/o adquisición. Este proceso se define como la recolección de los dispositivos y la documentación que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos. En séptimo lugar, la conservación/preservación. La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegro, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba. Y, en octavo y último lugar, la preservación de las evidencias digitales.

Por otro lado, se exige que los peritos tengan conocimientos científicos o artísticos necesarios para conocer o apreciar algunas circunstancias durante la instrucción de la causa, como así lo expresa el artículo 456 de la Ley de Enjuiciamiento Criminal. Según el artículo 457 del mismo cuerpo legal: «Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración. Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte».

El problema que se plantea en el caso de la pericial informática es que no existe una normativa de carácter nacional o internacional que determine la titulación o conocimiento necesarios para elaborar un dictamen de esta naturaleza. En España no existe todavía un Grado en Informática Forense, pese a que en algunos planes de estudio del Grado en Ciencias Criminológicas sí que encontramos asignaturas como informática forense o electrónica e informática forense. Pero lo más extendido es que la formación en esta especialidad se realice a través de distintos cursos impartidos por instituciones privadas donde se forma a los alumnos en las habilidades propias de esta materia. Estos cursos versan sobre la pericial judicial informática, derecho informático o peritaje telemático forense. En esta tesitura, surge la duda de qué titulación o conocimientos serían los adecuados para emitir un dictamen pericial informático.

En este sentido, Izquierdo Blanco(36) considera que lo más adecuado sería que el perito estuviera en posesión de un Grado en Informática, de Ingeniería (en todas sus acepciones, telecomunicaciones,

(36) Vid. Izquierdo Blanco, P., «Pericial informática. De acordarse una pericial informática, ¿qué titulación debe reunir el perito encargado de practicar la pericia, una licenciatura en informática, en ingeniería o en matemáticas», en Abel Lluch, X. y Picó I Junoy, J. (Dir.): *La prueba electrónica*, Colección de Formación Continua Facultad de Derecho ESADE, J. M. Bosch editor, Madrid, 2011, p. 409.

de sonido, imagen, etc.) o en Matemáticas, al tratarse de las disciplinas que guardan mayor conexión con la materia.

Sin embargo, se permite la intervención como peritos de personas que, sin ostentar una titulación oficial o académica, poseen conocimientos específicos en materia de informática forense adquiridos gracias a su experiencia personal o trayectoria profesional. En este caso, surgen interrogantes acerca de cómo determinar la experiencia mínima exigible a esa persona que carece de base académica que asiente sus conocimientos.

En el proceso penal, normalmente este tipo de pericias se realizan por las Brigadas Especializadas de las Fuerzas y Cuerpos de Seguridad del Estado. Son los agentes de determinadas unidades especializadas los que incautaran los dispositivos electrónicos que deben examinarse y efectúan, previa autorización judicial, el examen de estos en busca de evidencias del delito punible que sean objeto de investigación. En este sentido, las pericias podrán tener un objeto muy amplio y comprender, entre otros, el análisis de los intercambios de archivos, de *malware* instalado, del rastro dejado en la red para la comisión del delito, así como determinar el grado de conocimientos del presunto responsable para descartar otros posibles usuarios, técnicas de formateo o de cifrado de la información.

En el caso de la Policía Nacional, este tipo de investigaciones están centralizadas en la Unidad de Investigación Tecnológica (UIT)(37) dependiente de la Comisaría General de Policía Judicial. Dicha Unidad se subdivide en la Brigada Central de Investigación Tecnológica, a la que le corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones; y la Brigada Central de Seguridad Informática, dependientes ambas de la Comisaría General de Policía Judicial, a la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes.

En el caso de la Guardia Civil(38), las actuaciones de investigación y emisión de dictámenes periciales relacionados con la investigación de delitos cometidos a través de las tecnologías de comunicación se llevan a cabo por el Grupo de Delitos Telemáticos de la Unidad Central Operativa y en los Equipos de Investigación Tecnológica existentes en cada una de las provincias de España.

---

(37) Información disponible en http://www.policia.es/org_central/judicial/estructura/funciones.html

(38) Información disponible en https:// www.gdt.guardiacivil.es/webgdt/home_alerta.php

La pericial informática viene precedida de una investigación que consta de varias fases. En primer lugar, el análisis preliminar para la identificación de la prueba informática que se desea obtener, siendo aconsejable la implicación del perito desde el primer momento de selección de la información a identificar. En segundo lugar, la adquisición de los datos informáticos, proceso en el que es fundamental la conservación de las copias y la constatación de las técnicas empleadas para garantizar la integridad de la información. En esta fase, se recomienda que la prueba se obtenga a presencia de testigos o de un fedatario público y se deposite en soporte adecuado. Si se trata de una evidencia digital que se va a utilizar en un proceso civil, el depósito se podrá efectuar en una Notaría mediante la oportuna acta de manifestaciones del perito en la que detalle el proceso de obtención de la información. En el caso de tratarse de una evidencia digital que se va a utilizar en el proceso penal, se custodiará por el Letrado de la Administración de Justicia como pieza de convicción, sin perjuicio de que el Juez dicte las oportunas resoluciones para que los técnicos especialistas de las fuerzas de seguridad accedan a su contenido para emitir el dictamen pericial. Y, en tercer lugar, el análisis forense de la información digital, a cuyo efecto es conveniente que el perito, además de disponer de elevada formación y experiencia técnica, atesore un mínimo conocimiento de la normativa legal aplicable(39).

V. LA PERICIA COMO MEDIO DE PRUEBA E IMPARCIALIDAD DEL PERITO. ASPECTOS RELEVANTES DEL INFORME PERICIAL

La prueba pericial informática se practica a través de la aportación de un informe escrito en el procedimiento judicial. Este lo podemos definir como aquel medio de prueba a través del cual una persona emite una declaración de conocimiento sobre unos hechos, circunstancias o condiciones para lo que se requiere unos conocimientos científicos, artísticos, técnicos o prácticos.

La Ley de Enjuiciamiento Criminal regula los informes periciales tanto en la fase de instrucción (artículos 456 a 485) como en la fase de juicio oral (artículos 723 a 725). Dentro de dicha normativa, no se hace referencia específica a la pericial informática a diferencia de otros dictámenes periciales como, por ejemplo, la tasación pericial de objetos (artículo 365), informes periciales del Médico Forense sobre

(39) Vid. Pinto Palacios, F., Pujol Capilla, P.: *op. cit.*, p. 1.

edad del investigado (artículo 375) o informes periciales sobre muestras de ADN (artículo 363).

En el proceso penal, todo reconocimiento pericial se efectuará por dos peritos, según lo expresado en el artículo 459 en la Ley de Enjuiciamiento Criminal, siempre que sea un procedimiento ordinario o sumario (artículos 778 y 797 Ley de Enjuiciamiento Criminal). Para el procedimiento abreviado, el informe pericial podrá ser emitido por uno solo de ellos cuando el Juez lo considere suficiente (artículo 778.1 Ley de Enjuiciamiento Criminal). La exigencia de dos peritos ha sido matizada por la jurisprudencia en aquellos supuestos en los que el análisis pericial se realiza o por la Policía científica o por funcionarios de un laboratorio oficial, en el que se integra un equipo y el dictamen se basa en criterios científicos. Podemos citar la STS 10690/2004, de 17 de octubre, donde nos explica que «la exigencia de dualidad de peritos en cada dictamen pericial obedece a la mayor garantía de acierto que representa la posible coincidencia de pareceres de dos peritos frente a la opinión única, y a las mejores condiciones de objetiva valoración que para el Tribunal representan las posibles divergencias y opiniones encontradas de dos peritos intervinientes. De lo que se trata es de reforzar la eficacia, el acierto y el rigor técnico de los dictámenes periciales, sin que por ello se haga de la dualidad de peritos una condición inexcusable de la necesaria garantía puesto que el párrafo segundo del propio artículo 459 exceptúa el caso de que no hubiese más de un perito en el lugar y no fuera posible esperar la llegada de otro sin graves inconvenientes para el curso del sumario. En todo caso si el fundamento de la exigencia se halla en la mayor probabilidad de acierto que representa el trabajo realizado por varios, la finalidad de la norma queda satisfecha en el caso de dictámenes periciales emitidos por Órganos Oficiales dotados de equipos técnicos altamente cualificados integrados por distintos profesionales que intervienen como tales participando cada uno de sus miembros en el trabajo común dentro de la división de tareas o funciones. En tales casos el mero dato formal de estar suscrito el informe por uno solo de los profesionales del equipo, normalmente el que ejerce facultades representativas del Laboratorio u Órgano informante, como responsable o jefe del Servicio de que se trate, no puede ocultar el hecho real de que el dictamen no es obra de un solo individuo, es decir, de un perito, sino del trabajo de equipo normalmente ejecutado según procedimientos científicos protocolizados en los que intervienen varios expertos, desarrollando cada uno lo que le compete en el común quehacer materializado por todos. En estos casos no es que no sea aplica-

ble el artículo 459 de la Ley de Enjuiciamiento Criminal sino que debe entenderse satisfecha la exigencia que el precepto contiene».

Debemos señalar, que los peritos designados por el Juzgado de Instrucción pueden ser recusados a fin de garantizar su imparcialidad. Esta posibilidad queda limitada a aquellos supuestos en los que la prueba pericial no pueda reproducirse en el juicio oral (artículo 467 de la Ley de Enjuiciamiento Criminal). Las causas en que puede basarse la recusación son, en primer lugar, el parentesco de consanguinidad o de afinidad dentro del cuarto grado con el querellante o con el acusado. En segundo lugar, el interés directo o indirecto en la causa o en otra semejante. Y, en tercer lugar, la amistad íntima o la enemistad manifiesta.

Los informes periciales también pueden aportarse por las partes personadas en el proceso durante la fase de instrucción, así como acompañarlos junto con el escrito de calificación provisional (en el proceso ordinario; artículo 656 de la Ley de Enjuiciamiento Criminal) o en el escrito de acusación y/o defensa (en el proceso abreviado; artículos 781 y 784 de la Ley de Enjuiciamiento Criminal). De igual manera, también es práctica forense habitual aportar dichos informes periciales junto con la querella para justificar los hechos denunciados.

Una situación más complicada en las periciales aportadas por particulares o privadas es la validez de la prueba porque, en ocasiones, se producen injerencias, por ejemplo, en las telecomunicaciones entre particulares que afectan a la intimidad de terceros ajenos a la víctima y, por tanto, vulnerarían el derecho fundamental recogido en el artículo 18 de la Constitución.

Debemos tener en cuenta, en el caso de las pruebas informáticas que el elemento fundamental para la identificación de estas pruebas con respecto a aquellas obtenidas o aportadas por medios en los que no interviene la tecnología, es que contienen una serie de información conocida como metadatos. Estos son un grupo de datos ocultos que se almacenan en forma de ceros y unos y que exigen de su transformación en información legible y que describen el contenido informativo de un elemento digital y que, por tanto, aportan información adicional al archivo en el que se encuentren(40). Es decir, las pruebas tecnológicas contienen más información respecto a las que no tienen relación con las tecnologías de la información y de la comunicación.

Por otro lado, el artículo 336 de la Ley de Enjuiciamiento Criminal reconoce al investigado y su Letrado el derecho de asistir al reco-

(40) Vid. Perales Cañete, R.: «Exiftool: ¿Los metadatos sirven de algo?», en Oliva León, R; Valero Barceló, S. (Coord.): *La prueba electrónica. Validez y eficacia procesal*, Juristas con futuro, Zaragoza, 2016, p. 110.

nocimiento pericial de efectos que puedan tener relación con el delito. En el caso de los dispositivos de almacenamiento masivo de información y periciales sobre dispositivos informáticos en general, es obvio que se tiene esa facultad, porque la prueba que puede obtenerse de ellos está oculta, pudiendo solicitar un clonado de los dispositivos en ese momento. Aconseja siempre Martínez Galindo(41), que se acuda al acto de clonado y se solicite una copia para la defensa, para lo cual debe aportarse el oportuno dispositivo (que siempre tiene que ser nuevo o, en su caso, formateado y del doble de capacidad del que se va a copiar), a los efectos de que, en su caso, si se considera necesario, el investigado designe su propio perito para llevar a cabo otro reconocimiento pericial distinto.

En cuanto al objeto del informe pericial informático varía en función de las necesidades probatorias de los hechos investigados. Podemos distinguir entre las periciales que llevan a cambio auditorías de seguridad, periciales de autenticidad, de contenido, pericias de internet y aquellas que deben hacerse sobre los datos informáticos. También deberíamos tener en cuenta si se busca una peritación de un mero análisis de las comunicaciones, de la identificación de la dirección IP para determinar la procedencia de un ataque, o el origen del autor y el intercambio de datos o archivos. Ejemplo de ello, es en el caso de tener que buscar prueba a través del *blockchain*, debemos tener en cuenta que es un libro de contabilidad digital distribuido que almacena datos de cualquier tipo, desde transacciones de criptomonedas, propiedad de NFT(42) o contratos inteligentes DeFi(43). Por lo tanto, la complejidad de la peritación reviste tintes económicos y digitales.

En el informe pericial se tiene que explicar el motivo del análisis y el tipo de evidencias que han tratado de encontrar, así como la cronología del examen cibernético y las herramientas forenses utilizadas para el análisis de las evidencias. Las fuentes de información son los ordenadores, memorias, terminales móviles (en el caso de las criptomonedas se pueden tener aplicaciones en los dispositivos(44)), cada investigador crea su propia caja de herramientas cibernéticas (como, por ejemplo, herramientas de análisis de imágenes, de protocolos de

(41) Cfr. Martínez Galindo, G.: *Op. cit.*, p. 752.

(42) Las NFT o *Non Fungible Token* o *Tokens* no fungibles son un certificado digital de autenticidad que mediante la tecnología *blockchain*, la misma que se emplea en las criptomonedas (los tokens), se asocia a un único archivo digital.

(43) Los contratos inteligentes DeFi (contratos inteligentes de finanzas descentralizas) son una forma experimental de finanzas que no dependen de intermediarios financieros centrales.

(44) Algunas de las principales aplicaciones de criptomonedas son eToro, Capex, Markets.com, Plus500 o XTB.

red, de análisis de registros, para el cálculo de cash, entre otras) que irá actualizando en función de las necesidades de sus pericias.

La norma UNE 197010:2015 enumera los principios que deben respetarse durante la selección, obtención, presentación y almacenado de evidencias digitales: relevancia, fiabilidad, suficiencia y oportunidad. Pero también debemos tener muy presente la cadena de custodia de los mismo, la Circular 5/2019 de Fiscalía, en relación con las diligencias de investigación tecnológica, en su apartado 3.4.3 se refiere a la prueba pericial haciendo saber de la importancia de fijar las condiciones para asegurar la integridad de los datos y las garantías de su preservación. Se necesita garantizar la adecuada cadena de custodia de los efectos objeto de la pericia, asegurando que son los mismos y con el mismo contenido, con lo que fueron intervenidos. Se trata de garantizar la adecuada cadena de custodia de las fuentes de prueba, asegurando que lo que se analiza es justamente lo necesario para evidenciar el delito y que no ha sufrido alteración alguna.

Además de garantizar la identidad del objeto, la cadena de custodia cumple también la función de acreditar su autenticidad, pues asegura la imposibilidad fáctica de que el vestigio o prueba haya podido resultar manipulado o alterado(45). Según lo expuesto por Figueroa Navarro(46), y como crítica, considera necesario abordar la regulación normativa de la cadena de custodia de las fuentes de prueba, con el fin de unificar criterios de actuación y garantizar la corrección procesal en la obtención y aseguramiento de los vestigios delictivos.

El investigador forense puede visualizar el contenido de los datos en el momento de la investigación y descargar de la red o copiar a un fichero, disco duro o memoria USB, pero a los efectos de garantizar la pericial y su cadena de custodia debe acudirse a fedatarios públicos para certificar el contenido de la página web o aplicación, y generar un documento con el contenido completo de dicha web o aplicación, la fecha y la hora de la certificación y una firma electrónica que garantiza la integridad e inalterabilidad del documento, con la descarga de los archivos y ficheros, que deben quedar oportunamente reflejados en el acta que se levante y que constituyan indicios de delito.

Cuando el perito procede al análisis de las evidencias digitales se basa en analizar las pruebas electrónicas o cibernéticas y presentar la información en ellas de una manera objetiva y clara, sin que pueda dar

(45) Vid. Mestre Delgado, E.: «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en VV. AA.: *La cadena de custodia en el proceso penal,* Edisofer, 2015, p. 73

(46) Cfr. Figueroa Navarro, C.: «La cadena de custodia de las muestras biológicas», en VV. AA.: *La cadena de custodia en el proceso penal,* Edisofer, 2015, p. 127

lugar a la interpretación y puedan realizar valoraciones jurídicas, que les está vedado, toda vez que corresponde al Tribunal. En este sentido, y a modo de ejemplo, la STS 6007/2008, de 29 de octubre, delimita la función que corresponde al perito informático al establecer que «es evidente que la equiparación que efectúa el perito entre: ausencia de advertencia del programa Emule del sistema de archivos transparentes con la conclusión de que el usuario del programa desconocía y estaba ignorante de este dato no es admisible. Tal conclusión solo podría ser efectuada por el juzgador a quien le corresponde la tarea de valorar la actividad probatoria». En un sentido similar, se pronuncia la STS 406/2012, de 8 de noviembre, donde afirma que «no se pueden confundir los roles. El perito no puede suplantar ni al juez ni al testigo. Ni puede usurpar la función de valoración de la prueba que corresponde al Juez. Éste no puede convertirse en un mero espectador de la valoración realizada por los peritos».

Por último, señalar que el informe pericial puede ser presentado en cualquier fase del procedimiento, pero en cada una de ellas despliega distintos efectos, por la naturaleza de cada fase y los fines que se persiguen. Ciertamente, en materia de Criminalidad Informática tiene su ubicación más adecuada en la fase de instrucción del proceso, ya que será determinante y esclarecedora tanto para averiguar la ejecución del delito como la concreta identidad del delincuente. De hecho, si ponemos como ejemplo nuestro delito objeto de estudio, el blanqueo de capitales a través de las criptomonedas, deberemos aportar informes periciales que acrediten la relación de actuaciones con los presuntos responsables (ya sean personas físicas o jurídicas). Esta información se efectuará por peritos privados y será adjuntada a la querella o denuncia que se presente.

Los informes periciales practicados durante la fase de instrucción no constituyen pruebas, sino solo diligencias de investigación para determinar si existen elementos suficientes de determinación de la autoría, y para que puedan constituir verdadera prueba deben ser ratificados en Juicio Oral. Es en esta fase donde se procede a su valoración judicial. En este sentido, el artículo 741 de la Ley de Enjuiciamiento Criminal establece que el Tribunal dictará sentencia valorando «según su conciencia las pruebas practicadas en el juicio». La jurisprudencia ha declarado que ello supone que la prueba se debe valorar sin sujeción a tasa, pauta o regla de ninguna clase, para evitar cualquier tipo de arbitrariedad por los poderes públicos, es decir, por los Juzgados y Tribunales. Es necesario que en la sentencia se desarrolle la argumentación que sostiene la valoración de la prueba que, en todo caso, deberá ajustarse a las reglas de la lógica, la racionalidad y

la coherencia. En consecuencia, la prueba pericial informática se valora por el Tribunal según las reglas de la sana crítica atendiendo al resto de medios de prueba que se hayan practicado en las sesiones de juicio oral. Dado que en el proceso penal las únicas pruebas que pueden desvirtuar la presunción de inocencia, según el artículo 24.2 de la Constitución Española, son aquellas que se practican en el juicio oral con las garantías de publicidad, oralidad, inmediación y contradicción, se han planteado algunos problemas prácticos cuando el perito no comparece en el juicio oral para ratificar su informe. La regla general es que el perito informático deberá comparecer personalmente al acto del juicio para exponer, ampliar siempre que no se sobrepasen los límites del objeto de la pericia, o aclarar lo que se estime oportuno en el plenario respecto del contenido del informe emitido.

La jurisprudencia del Tribunal Constitucional (SSTC 127/1990 y 24/1991) y del Tribunal Supremo (STS 62839/2011, de 24 de mayo) han manifestado que, si bien la prueba pericial debe ser practicada en el acto del juicio oral, puede ocurrir que, aportada durante la fase de instrucción y conocida por las partes al tiempo de emitir su escrito de calificación, si nadie formula impugnación o propone la comparecencia del mismo al acto del juicio, puede estimarse que existe una aceptación tácita de su resultado. De esta manera, el Tribunal podrá valorar ese dictamen como auténtico medio de prueba, aun cuando el perito no haya comparecido a juicio, máxime si el informe pericial ha sido realizado por un órgano de carácter público u oficial(47).

VI. CONCLUSIONES

El incremento de los delitos ciberdelincuentes en los últimos años es evidente. En parte se debe al aumento progresivo que existe del uso de las tecnologías en todos los ámbitos. Esto significa que, al igual que la sociedad ha entrado y explorado el mundo *online* y *offline*, los delincuentes también lo han hecho.

Como hemos podido plasmar, las criptomonedas y su frenética fenomenología constituyen una innegable fuente de riesgos penales. Sin lugar a dudas, el que mayor atención a suscitado es su posible uso ilícito y como forma para introducir activos procedentes de actividades delictivas en la economía legal. Además, hay que añadir que ninguna criptomoneda, descentralizada o centralizada, goza de ser

(47) Vid. Pinto Palacios, F., Pujol Capilla, P.: *La prueba en la era digital,* La Ley, Madrid, 2017, p. 200

moneda de curso legal en la Unión Europea. Si algún Estado, cuya moneda sea el euro, llegase a formar la intención de legislar para considerarla como moneda de curso legal, dicho Estado podría hacerlo únicamente en desarrollo de la normativa que a ese respecto marcase la Unión Europea, la cual dispone de competencia exclusiva sobre la política monetaria de los Estados miembros cuya moneda es el euro (artículo 3 del Tratado de Funcionamiento de la Unión Europea).

Como se mencionó anteriormente, las criptomonedas tienen ciertas características que las hacen atractivas para su uso fraudulento, especialmente en el delito de blanqueo de capitales, como la dificultad para asociar direcciones de envío y de recepción de criptomonedas o la imposibilidad de atribuir un identificador único, entre otras.

Estas conductas delictivas cibernéticas no sólo son novedosas en la legislación penal sino también a la hora de evidenciar este tipo de delitos contra el patrimonio y el orden socioeconómico, entre otros, mediante la prueba, de ahí la importancia y auge de la prueba pericial informática, y a su vez, la figura del perito y su informe. Estos son necesarios para aportar el conocimiento técnico, en este caso, sobre las conductas ciberdelincuentes, y bajo la objetividad de sus aportaciones, de ayuda a la valoración por parte del Juez.

VII. BIBLIOGRAFÍA

Arrabal Platero, P.: La prueba tecnológica: aportación, práctica y valoración, Tirant lo Blanch, Valencia, 2019.

Banco Central Europeo: «Virtual currency schemes: A further analysis», Frankfurt am Main, 2015 Disponible en: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Barroilhet Díez, A.: «Criptomonedas, economía y derecho», en Revista chilena de derecho y tecnología, Vol. 8, núm. 1, 2019.

Cerezo Domínguez, A. I. «La ciberdelincuencia en España: un estudio basado en las estadísticas policiales», en *Revista de Estudios Penales y de la Seguridad* núm. 6, 2020.

Fernández Bermejo, D. (Dir.): *Blanqueo de capitales y TIC: Marco Jurídico y Europeo, Modus Operandi y Criptomonedas,* Thomson Reuters Aranzadi, Cizur Menor, 2019.

Figueroa Navarro, C.: «La cadena de custodia de las muestras biológicas», en VV. AA.: *La cadena de custodia en el proceso penal,* Edisofer, 2015.

Gimeno Sendra, V.: l, Derecho Procesal Civil I: El Proceso De Declaración. Parte General, Ediciones Jurídicas Castillo de Luna, Madrid, 2015.

Izquierdo Blanco, P., «Pericial informática. De acordarse una pericial informática, ¿qué titulación debe reunir el perito encargado de practicar la pericia, una licenciatura en informática, en ingeniería o en matemáticas», en Abel Lluch, X. y Picó I Junoy, J. (Dir.): La prueba electrónica, Colección de Formación Continua Facultad de Derecho ESADE, J. M. Bosch editor, Madrid, 2011.

Martínez Galindo, G.: «La prueba pericial informática y tecnológica», en VV. AA.*: Tratado de Delincuencia Cibernética,* Thomson Reuters Aranzadi, Cizur Menor, 2021.

Mestre Delgado, E.: «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en VV. AA.: *La cadena de custodia en el proceso penal*, Edisofer, 2015.

— «Introducción», en VV. AA.: Tratado de Delincuencia Cibernética, Thomson Reuters Aranzadi, Cizur Menor, 2021.

Morales García, O.: «Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información», en *Cuadernos de Derecho Judicial* núm. 9, 2002.

Muñoz Machado, S.: *La regulación de la red. Poder y Derecho en Internet,* Taurus, Madrid, 2000.

Nakamoto, S.: «Bitcoin: A Peer-to-Peer Electronic Cash System», en bitcoin.org. Disponible en: https://bitcoin.org/bitcoin.pdf

Nieto Martín, A., García-Moreno, B.: «Criptomonedas y derecho penal: más allá del blanqueo de capitales», en *Revista Electrónica de Ciencia Penal y Criminología,* 23-17, 2021, p. 4. Disponible en: http://criminet.ugr.es/recpc/23/recpc23-17.pdf

Perales Cañete, R.: «Exiftool: ¿Los metadatos sirven de algo?», en Oliva León, R; Valero Barceló, S. (Coord.): *La prueba electrónica. Validez y eficacia procesal, Juristas con futuro,* Zaragoza, 2016, p. 110.

Pérez López, X.: «Las criptomonedas: consideraciones generales y empleo de las criptomonedas con fines de blanqueo», en Fernández Bermejo, D. (Dir.): *Blanqueo de capitales y TIC: Marco Jurídico y Europeo, Modus Operandi y Criptomonedas,* Thomson Reuters Aranzadi, Cizur Menor, 2019.

— «El blanqueo de capitales a través de las criptomonedas», en VV. AA.: *Tratado de Delincuencia Cibernética,* Thomson Reuters Aranzadi, Cizur Menor, 2021.

Pinto Palacios, F., Pujol Capilla, P.: «La prueba pericial informática», en Diario La Ley, núm. 5, Sección Ciberderecho, 3 de abril de 2017, p.1. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1CTEAAiMTEyMTS7Wy1KLizPw8WyMDQ3MDEwNjkEBmWqVLfnJIZUGqbVpiTnEqAJMEEw1AAAAWKE

Pinto Palacios, F., Pujol Capilla, P.: *La prueba en la era digital,* La Ley, Madrid, 2017.

Velasco Núñez, E.: «Ciberseguridad, ciberdelincuencia y empresa: la respuesta penal», en *Revista de privacidad y derecho digital,* Vol. 4, núm. 14 (abril-junio), 2019.