CRIPTOACTIVOS: INVESTIGACIÓN Y ASEGURAMIENTO EN DELITOS

CRIPTOASSETS: CRIME INVESTIGATION AND SEIZURE

ELOY VELASCO NÚÑEZ*

RESUMEN

Los criptoactivos han entrado en la categoría de "instrumentos financieros". La importancia del presente trabajo radica en la necesidad de la regulación de estos criptoactivos. Aunque existe la regulación pública de algunas modalidades de criptoactivos, la mayoría todavía permanecen al margen de las leyes, únicamente diseñadas por sus algoritmos rectores. La transformación digital está operando en los delitos económicos. El objetivo central del presente trabajo consiste en analizar los retos que se presentan en la procuración y administración de justicia en los delitos vinculados con los criptoactivos, tanto en la investigación y el aseguramiento, así como otros aspectos procesales. Para lo anterior se ha aplicado el método analítico de diversas fuentes jurídicas españolas y europeas. Se concluye que existen diversas medidas restrictivas para elegir la idónea. Además, ciertas actuaciones sobre esta pueden servir de prevención delictiva o como aseguramiento de una futura posible sanción contra un posible infractor económico tecnológico.

PALABRAS CLAVE: criptoactivos, investigación en delitos, aseguramiento en delitos.

ABSTRACT

Cryptoassets have entered the category of "financial instruments."

*Magistrado de la Audiencia Nacional de España.

The importance of this work lies in the need to regulate these cryptoassets. Although some types of cryptoassets are publicly regulated, most still remain outside the law, designed solely by their governing algorithms. The digital transformation is operating in economic crimes. The main objective of this work is to analyze the challenges that arise in the prosecution and administration of justice in crimes related to cryptoassets, both in investigation and prosecution, as well as other procedural aspects. To this end, the analytical method of various Spanish and European legal sources has been applied. It is concluded that there are various restrictive measures to choose the most appropriate one. Furthermore, certain actions regarding these measures can serve as crime prevention or as a guarantee of a possible future sanction against a potential economic and technological offender.

KEYWORDS: cryptoassets, crime investigation, crime seizure.

1. CUESTIONES INTRODUCTORIAS: CONCEPTO Y CARACTERÍSTICAS:

Los criptoactivos[1] [2] [3] son representaciones digitales de valor/derechos que pueden transferirse/almacenarse electrónicamente, mediante tecnología de registro distribuido o similar.

---

[1]Comisión Nacional del Mercado de Valores, «Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión», Pub. L. No. Circular 1/2022, § 1, BOE-A-2022-666 4106 (2022), https://www.boe.es/eli/es/cir/2022/01/10/1.; Reglamento UE 2022/1114 del Parlamento y del Consejo, relativo a los mercados de criptoactivos, en adelante MiCA y, en lo que se refiere a su cristalización más conocida, las criptomonedas, el Art. 1.5 L. O. 10/2010, de 28 de abril, de prevención del blanqueo de capitales y financiación del terrorismo.

[2]«Reglamento (UE) 2023/ del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.o 1093/2010 y (UE) n.o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937», s. f. Art. 3.1.5.

[3]«Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.», Pub. L. No. BOE-A-2010-6737 (2010), https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737. , en lo que se refiere a su cristalización más conocida, las criptomonedas, el Art. 1.5.

La tecnología DLT (de registro distribuido) que les sirve de base son sistemas electrónicos o bases de datos que permiten registrar, almacenar y distribuir información descentralizadamente, tanto de forma privada como pública, que pueden estar conectados entre sí y que requieren de una red de igual a igual (peer to peer), así como de algoritmos de consenso que garanticen la replicación entre sus nodos. El sistema Blockchain, que puede ser público o privado, y usa forma de diseño de libro mayor distribuido, es el más conocido.

Aunque la aplicación práctica más popular de los criptoactivos son las criptomonedas —y entre ellas, la más conocida, el bitcoin—, los primeros constituyen un término más amplio, que no sólo abarca las criptomonedas, sino también otras representaciones digitales de valor —tokens de seguridad, NFTs …—, que usan también la criptografía para asegurar sus transacciones.

Se trata de elementos inmateriales representativos de valor que sus usuarios aceptan y que se expresan criptografiados, -a través de algoritmos codificados para proteger y ocultar la información transmitida para que solo pueda ser leída por aquellos con permiso y capacidad de descifrarla-, de ahí parte de su nombre.

En el caso de las criptomonedas, aunque normal y mayoritariamente son de carácter privado, puede también haberlas emitido la Autoridad pública —como es el caso de los CBDCs[4]—, e igualmente, aunque no suelen estar asociadas a una moneda fiduciaria, pueden estarlo, como es el caso de los EMTs (electronic money tokens/fichas de dinero electrónico, regulados en el Título IV del Reglamento MiCA, Arts. 48-58) y ARTs (assets referred to tokens/fichas referenciadas a activos, regulados en el Título III del Reglamento MiCA, Arts. 16-47).

[4]CBDC (Central Bank Digital Currency): según el Banco de España, es una nueva forma de dinero emitida de forma electrónica por un banco central. Los bancos centrales buscan emitir sus propias monedas digitales con el objetivo de mejorar el sistema de pagos, dado el aumento de los pagos electrónicos y el descenso del uso del efectivo, pero también porque la creación de instrumentos electrónicos de pago privados no regulados, como las stablecoins, puede poner en riesgo la estabilidad financiera. En julio de 2021, el Consejo de Gobierno del Banco Central Europeo (BCE) decidió poner en marcha el proyecto de un euro digital.

Como representación de valor que encarnan, pueden usarse como: medio de intercambio, como inversión, o para acceder a un bien/servicio.

Como medio de pago (depósito de valor y unidad de cuenta), distinto del efectivo —moneda o billete estatal de curso legal—, se les denomina criptomonedas, o monedas virtuales que son "representaciones digitales de valor no emitidas o garantizadas por un Banco central o Autoridad pública, no necesariamente asociadas a una moneda legalmente establecida y que no poseen estatuto jurídico de moneda o dinero, pero que son aceptadas como medio de cambio y pueden ser transferidas, almacenadas o negociadas electrónicamente" (RDL 7/21, que traspone la quinta Directiva europea de prevención de blanqueo de capitales y financiación del terrorismo).[5]

De ellas hay en la actualidad aproximadamente más de 10.000 diferentes en el mercado mundial, casi todas de carácter privado, y transaccionan más de 112.000 millones de dólares al año, valiendo el 0´59 % del dinero fiat mundial,[6] equivaliendo al 0´23 % del dinero en el mundo.

Las Plataformas tecnológicas que operan con criptomonedas reciben el nombre acrónimo de VASP/CASP (Virtual/Cripto Assets Service Providers), y aunque el Reglamento MiCA las clasifica en diversas categorías (emisoras: de fichas referenciadas a activos y de fichas de dinero electrónico; proveedoras de servicios[7]), normalmente se las denomina "Exchange" si se dedican prioritariamente al intercambio de cripto por dinero fiat y "Wallet", si a la gestión de monederos virtuales y criptos.

[5]Definición que, tras la aparición de las CBDCs, obviamente, debe revisarse.
[6]Businessinsider.es: Cuánto suponen las criptomonedas del total del dinero del mundo.
[7]Ver Directiva 2014/65/UE): de custodia y administración de criptoactivos por cuenta de clientes; de gestión de plataforma de negociación de criptoactivos; de canje de criptoactivos por fondos y otros criptoactivos; de ejecución de órdenes relativas a criptoactivos por cuenta de clientes; de colocación de criptoactivos; de recepción y transmisión de órdenes relativas a criptoactivos por cuenta de clientes; de prestación de asesoramiento en materia de criptoactivos y de prestación de servicios de gestión de carteras de criptoactivos.

Ya hemos señalado que este mercado está mayoritariamente centrado en el sector privado, y dentro de él, lo suelen servir empresas -financieras: bancarias o no- proveedoras de servicios de criptos que deben necesariamente registrarse en el Banco de España, cumplir exigentes requisitos de publicidad y gestión señaladas en el Reglamento MiCA (para los tokens de utilidad —utility tokens[8]—, los referenciados a activos/ART[9] y los de dinero electrónico —EMT/e-money tokens[10] —), o en la Directiva MIFID[11] (para los tokens de inversión —security tokens—), así como a la CNMV en cuanto a su emisión, y por supuesto, a la regulación en prevención del blanqueo de capitales y financiación del terrorismo.

Los primeros años de desarrollo privado de los criptoactivos, en especial las criptomonedas-, han ido presentando una serie de riesgos económicos que poco a poco se han ido corrigiendo/mitigando, y que eran:

- Alta volatilidad, con enormes fluctuaciones de valor en el tiempo a la hora de su conversión —voluntaria, no obligatoria— en moneda fiat o de curso legal
- Escalabilidad operativa lenta (son incapaces de hacer en un determinado tiempo las mismas transacciones que Visa o Mastercard)
- Escasa ecología por su alto consumo de energía
- No respaldo gubernamental, careciendo de mecanismos de protección (tipo Fondo de Garantía de Depósito), ni

[8] Título 2 Reglamento MiCA: otorgan a su poseedor acceso a un producto o servicio basado en un sistema Blockchain en una plataforma digital.

[9] Título 3 Reglamento MiCA: otorgan derecho de propiedad, uso o acceso al activo/s, tangible o no, público o privado, a que se vinculan.

[10] Título 4 Reglamento MiCA: dinero electrónico

[11] Diario Oficial de la Unión Europea, «Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE» (s. f.), https://www.boe.es/doue/2014/173/L00349-00496.pdf.

de subyacente físico de respaldo, lo que no significa que no tengan protección legal, en el caso de la Unión Europea. En el mundo, hay:

Países que admiten alguna cripto privada como moneda de curso legal (i. e: El Salvador y República centroafricana),

Aquellos en que, no siendo de curso legal, admiten transaccionar con ellas (i. e: España; EE. UU.; Argentina; México…)

Los que las imponen restricciones bancarias (i. e: Colombia, Canadá…)

Los que las prohíben como medio de pago: (i. e: Vietnam, Arabia Saudí…) y

Los que las han declarado ilegales: (i. e: China, Bolivia…)

- No cuentan con un gestor intermediario ni responsable de las operaciones, que están automatizadas, de manera que su asunción y uso depende de la confianza que le otorguen sus usuarios.
- No son medio de pago legal (salvo en El Salvador —desde el 9/06/2021— y República Centroafricana —desde el 23/04/2022—), de manera que son activos virtuales que no generan la obligación de ser aceptados universalmente.

Pero este panorama inicial y muy específico del Bitcoin, lleva cambiando sustancialmente en los últimos años.

Por una parte, los criptoactivos han entrado también en la categoría de "instrumentos financieros" cuando se negocian como contrato de apoyo a la inversión que da lugar a un activo financiero para el tenedor y un pasivo o instrumento de patrimonio para el emisor.

Y por otro, a la incorporación en cuanto a su gestión de muchas entidades bancarias y financieras clásicas, se han ido sumando elementos y mejoras que han incrementado su confianza:

- La gestación de Stablecoins, (tipo Tether, TrueCoin o DAI), esto es, de monedas virtuales con mecanismos de

estabilización de su valor/precio —colateralización— para reducir su volatilidad al estar asociadas, —respaldadas, tokens/fichas referenciadas o ARTs— por 1) el valor de bienes externos/materiales: como pueden ser otras monedas fiat -euro/dólar-, materias primas como metales —oro, plata— o inmuebles o 2) el de otra criptomoneda, o 3) a una cesta mixta de las anteriores, o incluso a 4) algoritmos (i. e: USDX) que mantienen su precio estable, reduciendo enormemente sus fluctuaciones de valor, gracias a incentivos programados algorítmicamente en los que el smart contract[12] actúa de Banco central ajustando el valor de la oferta y la demanda.

- La aparición de las monedas digitales estatales (CBDCs), -representación digital de moneda fiat, o fiat digitalizado, tokenizado como activo virtual regulado por los Estados-emitidas y respaldadas por organismos oficiales públicos, los Bancos centrales, como el euro, dólar, yuan o rublo digitales… que suman mecanismos de respaldo subyacente y protección garantizados por la Autoridad Pública, de manera que alejan el peligro de insolvencia.
- Escalabilidad cada vez mayor, gracias a la implantación en sus cadenas de bloques de "sidechains" —o cadenas laterales— que proporcionan una mejor escalabilidad —velocidad a la hora de hacer sus transacciones— porque descargan ciertos cálculos o transacciones de la cadena principal en una cadena separada que alivia la congestión y reduce la carga en la red principal.
- Regulación pública de algunas modalidades de criptoactivos, ya que pese a que la mayoría todavía permanecen

[12] Acuerdos de voluntades informatizados y autoejecutables (no necesitan en su ejecución intervención humana alguna) que usan tecnología blockchain. Para cada supuesto de hecho –cumplimiento/incumplimiento de circunstancia-, prevé una concreta consecuencia jurídica previamente determinada, que se autoejecuta.
Características: autoejecutabilidad; inmodificabilidad; seguridad; confianza.

al margen de las leyes, únicamente diseñadas por sus algoritmos rectores, la Unión Europea, conformada por 27 países, ha sometido a legislación (el Reglamento (UE) MiCA, 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos) a los ARTS ("un tipo de criptoactivo que no es una ficha de dinero electrónico y que pretende mantener un valor estable referenciado a otro valor o derecho, o a una combinación de ambos, incluidas una o varias monedas oficiales"), los EMTS ("un tipo de criptoactivo que, a fin de mantener un valor estable, se referencia al valor de una moneda oficial") y los utility tokens o fichas de consumo ("un tipo de criptoactivo utilizado únicamente para dar acceso a un bien o un servicio prestado por su emisor").

- Ecología, por cuanto modificaciones en su sistema de consenso, pasando del modelo de prueba de fuerza —proof of forcé—- tan consumista de energía, hacia los de prueba de bloqueo —proof of stake— que, al validar las transacciones mediante consensos restringidos, consumen mucha menos, volviéndolas mucho más conservacionistas.

Medidas cambiantes y evolución hacia su mejora y reducción de riesgos que, en definitiva, han aumentado tanto su confiabilidad que han llevado a instituciones bancarias clásicas a entrar en ese mercado potenciando igualmente el número de sus usuarios habituales.

2. CREACIÓN, OFERTA, DESARROLLO Y TRANSACCIÓN DE CRIPTOACTIVOS

Desde la perspectiva penal que nos ocupa, nos centraremos en las diferentes maneras de obtenerlos ilícitamente, analizando los momentos en que los criptoactivos son atacados durante sus fases de creación, oferta y desarrollo como inversión y transacción, en donde se están generando ya actuaciones delictivas.

En la fase de la creación del criptoactivo —aparte el cumplimiento administrativo de las imposiciones previstas por el Reglamento MiCA 2013/1114, cuya exigencia evitará en el territorio de la Unión Europea la entrada en este mercado de operadores que no alcanzan categoría adecuada para hacerlo— podemos plantearnos si cabe que la emisión dañina de criptoactivos —singularmente criptomonedas— no autorizadas, pueda ser sancionada penalmente como delito de peligro abstracto —infracción administrativa de entidad, criminalizada—.

Desde luego, en las inversiones sobre ICOs[13] y en la creación de criptoactivos, podría sancionarse penalmente al emisor que, con intención de perjudicar económicamente -ya que siempre supone una reducción de valor-, acuñe más ejemplares de lo informado, o prepare actuaciones de pre minado ocultando, incluso en connivencia/acuerdos con grupos reducidos de mineros, la existencia y puesta en circulación de más ejemplares de los informados, o a quien mediante interferencias tecnológicas -hackeos, adiciones de datos…- cree inconsentidamente más ejemplares no conocidos.

En la fase de la oferta el Derecho Penal debería estar atento a la información engañosa que se pueda llevar a cabo en la presentación de la inversión, singularmente fijándose en los rendimientos ofrecidos, —para evitar estafas piramidales con esquema tipo Ponzi—, para lo cual se debe analizar la omisión de información necesaria (whitepapers) antes de lanzar el producto, la aparición de falsas criptomonedas (scamcoins), la intervención de falsos intermediarios —participación delictiva— y el desarrollo de su propia publicidad, en especial la de su rendimiento, con incluso el reclamo de personajes famosos o mediante redes conocidas para alterar su precio/valor.

En la fase de la inversión y transacción, por su parte, además de los apoderamientos engañosos al intercambiar/negociar, el Derecho Penal deberá sancionar a quien recibiendo billeteras/monederos para ser gestionados por expertos, deslealmente se apodere inconsentidamente de todo o parte de su contenido, inversión o transacción.

[13] Initial Coin Offer: oferta inicial de moneda.

En el intercambio o gestión externa de criptoactivos, las normas no deben incidir en el software, ni en la tecnología subyacente —pues es un aspecto que debe permanecer neutral—, sino sobre las acciones humanas, en nuestro caso antijurídicas, vinculadas al propio producto, analizando la forma en que quienes los usan, aunque no sean CASP y sí DeFI, llevan a cabo el control de su gestión y trasvase.

El intercambio/gestión de criptoactivos pueden hacerlo entidades centralizadas y descentralizadas.

Simplificando, entre las centralizadas encontramos empresas que realizan cambio de moneda virtual por moneda fiduciaria: «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 cambio en el país en el que se haya emitido», y proveedores de servicios de custodia de monederos electrónicos: «aquellas personas físicas o jurídicas que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales».

En el sector DeFI (finanzas descentralizadas), a través de Plataformas de intercambio descentralizado (DEX), en el mercado de intercambio P2P se pone en relación con compradores con vendedores, transaccionando ellos y no las empresas, cada cual, con sus claves y billeteras, sin intermediarios y mediante contratos inteligentes autoejecutables.

En estas últimas, la labor más técnica de intermediación de las empresas, sin embargo, no debe relajar el cumplimiento de las exigencias del protocolo conoce a tu cliente "KYC" en materia de prevención y denuncia por sospecha de delito de blanqueo de capitales.

3. DELITOS VINCULADOS A LOS CRIPTOACTIVOS

La propia transformación digital y el trasvase del manejo físico hacia el virtual de los activos —no sólo del dinero— está a su vez modificando la conducta delictiva económica, y con ella su respuesta penal.

La principal transformación está operando en los delitos económicos de apoderamiento, en el que la estafa, que en el mundo

físico ponía su acento penal en el engaño para generar o mantener a la víctima en un error que posibilitase una transferencia económica perjudicial en su contra, se está pasando hacia un concepto más genérico de fraude vinculado a la obtención/causación torticera, inconsentida, inconsciente, de perjuicio patrimonial, esto es, a procurarse un provecho económico irregular/ilícitamente, sólo que sobre activos digitales o su representación de valor.

Cuando se analiza la incidencia que ello genera en la nueva economía de los intangibles, sobre los nuevos valores digitalizados, los tokens, y sus representaciones -de valor y monetarios-, nos interesa no sólo recalcar que a partir de la entrada en vigor de la reforma llevada a cabo por L. O. 14/2022 de 22 de diciembre el 12/01/2023,[14] no hay duda de su protección penal, pues como patrimonio, son activos -predicándoseles, en consecuencia la protección de los delitos económicos, incluida la del Art. 248 CP-, y como criptomonedas, son medios de pago, protegiéndose además la confianza especial en ellos y en esa función que impone como nuevo bien jurídico protegido el Art. 249 CP.

Como objeto delictivo, el criptoactivo puede ser producto de la estafa —i. e: pretender cambiarlo en falsas Exchanges que se apropian de él— como lo es también el denominado "robo" de los monederos virtuales que los contienen, que el Art. 249.2.b CP considera específicamente una defraudación y no propiamente una gestión desleal/apropiación indebida de criptoactivos.

Estos se producen cuando el administrador custodio de la billetera virtual de su cliente, anteponiendo su propio interés o dando preferencia a unas órdenes frente a otras, se adelanta a comprar o a vender a precio mayor determinados criptoactivos, sin conocimiento del cliente y contraviniendo los deberes de diligencia que impone el Art. 221 Ley Mercado de

[14] Jefatura del Estado, «Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso.», BOE-A-2022-21800 § (2023), https://www.boe.es/buscar/act.php?id=BOE-A-2022-21800.

Valores, RDL 4/2015, de 23 de octubre,[15] apoderándose de la diferencia económica/ganancia a favor, que oculta a su administrado.

También como objeto delictivo, solo que más sofisticado, están los hackeos tecnológicos orientados al apoderamiento de billeteras virtuales que con el oportuno cambio de clave privada suponen el apoderamiento del propio activo virtual (tipificable como estafa tecnológica del Art. 249.1.a CP y no como robo, pues su forma/*modus operandi* comisivo es la manipulación/artificio tecnológico) que se consiguen aplicando artimañas tecnológicas —i. e: clonación del SIM de una tarjeta telefónica…— dirigidas a hacerse con las claves privadas del monedero virtual, o incluso el ataque tecnológico a las propias Plataformas gestoras de los mismos —puertas traseras, *man in the middle*...— para apoderarse de sus monederos.

En segundo lugar, si alcanzaran la categoría de "instrumentos financieros" definidos en la D 2014/65/UE MiFID —lo que parece improbable a la luz de su Art. 4.1º.15 DMiFID—, o al menos en el caso de los considerados como producto "asimilado" a inversión regulados en los Arts. 76-80 del Reglamento MiCA —y no hay duda de que muchos usuarios los acopian como inversión para especular en el futuro, empleándolos como medio de ahorro—, deberían protegerse mediante ciertos delitos contra el mercado —no sólo financiero— y los consumidores como podrían ser la alteración de precios del Art. 284 CP, la publicidad engañosa del Art. 282 CP, las estafas de inversión del Art. 282 bis/288 CP, o incluso el abuso/manipulación de mercado mismo cuando su gestor lleve a cabo manipulaciones —i. e: inventar o hacer intervenir a compradores ficticios—

[15]«Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores.», BOE-A-2015-11435 § (2015), https://www.boe.es/buscar/act.php?id=BOE-A-2015-11435.

para incrementar artificiosamente el valor de lo que se ordene comprar; o realizar operaciones simuladas para alterar/mantener el valor del activo o cuando utilice información privilegiada especulativamente (Art. 285 CP).

Igualmente, los activos digitales y su capacidad de ser transaccionables electrónicamente, les hace aptos para ser instrumento de pago a la vez que de posible encubrimiento de previas actividades delictivas (blanqueo de capitales) o contra la normativa de control de cambios.[16]

Nos referimos, singularmente, a las transacciones económicas que se están tratando con los denominados fusionadores o difuminadores (merge), mezcladores de transacciones electrónicas (i. e: Tornado Cash) que impiden rastrear los destinatarios, ofuscando/camuflando los activos tras una defraudación.

Por otra parte, han aumentado los controles administrativos que permiten operar en el mercado de criptoactivos no sólo gracias al Reglamento MiCA, sino igualmente mediante el Reglamento ToFR 2023/1113[17] relativo a la información que acompaña a las transferencias de fondos de determinados criptoactivos, imponiendo la denominada travel rule, exigencia del GAFI que obliga a los proveedores de servicios con criptomonedas e instituciones financieras a compartir con las Autoridades competentes "información relevante" sobre el originador y el beneficiario de cada transacción en que operen con criptoactivos para evitar el blanqueo/lavado con estos, de manera que la información sobre el origen del activo y su beneficiario deben viajar con la —información de la— propia transacción y almacenarse en ambos lados de la transferencia.

[16] Ley 40/1979, de 10 de diciembre, sobre régimen jurídico de control de cambios, en lo que no sea inconstitucional.

[17] Unión Europea, «Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.», BOE.es - DOUE-L-2023-80807 § (2023), https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80807.

De esta forma se obtendrá, retendrá y transmitirá de manera segura la información sobre quien la origine y el beneficiario que la reciba al realizar transferencias.

Por su parte la AEVM (Autoridad Europea de Valores y Mercados) debe llevar un Registro público de las CASP no autorizadas para prestar servicios en la UE, de manera que se vaya aislando a las plataformas Exchange/Wallet que operan fuera del territorio de la Unión Europea, a veces creadas ex professo para burlar las exigencias comunitarias de cumplimiento normativo y de prevención del blanqueo de capitales, ya que en el territorio común de los 27 EM las CASP están obligadas a aplicar idénticas medidas preventivas que las instituciones financieras —el protocolo KYC: identificar al usuario, al titular real, conocer el origen de sus fondos, verificar la realidad de su actividad de procedencia...—, incluida la debida diligencia respecto del cliente, el mantenimiento de registros y la notificación de transacciones sospechosas (5ª Directiva PBC/FT, 2018/843, traspuesta mediante RDL 7/21, de 27 abril 21[18] y 6ª Directiva PBC/FT, 2018/1673 traspuesta en la oportuna reforma del CP mediante L. O. 6/2021, de 28 de abril[19]) ya que son sujetos obligados.

El futuro Reglamento (UE) que ya se prepara en materia de protección frente al blanqueo de capitales y financiación del terrorismo (AMLR) parece pretender la prohibición de

[18] Jefatura del Estado, «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.», BOE-A-2021-6872 § (2021), https://www.boe.es/buscar/act.php?id=BOE-A-2021-6872.

[19] Jefatura del Estado, «Ley Orgánica 6/2021, de 28 de abril, complementaria de la Ley 6/2021, de 28 de abril, por la que se modifica la Ley 20/2011, de 21 de julio, del Registro Civil, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.», BOE-A-2021-6944 § (2021), https://www.boe.es/buscar/act.php?id=BOE-A-2021-6944.

las transacciones económicas anónimas con criptoactivos (por ir contra la travel rule), las cuentas anónimas y criptos de mejora del anonimato (tipo Monero o ZCash), así como las billeteras sin custodia (autoalojadas), de manera que quedarán fuera de su ámbito de regulación las transacciones peer to peer entre particulares (sin intervención alguna de CASPs), los billeteros autoalojados (tipo Trezor o Metamask), y aquellas operaciones con criptos en que intervengan los proveedores de servicios vinculados a NFTs, DeFI/DAO y Metaversos.

Además, los criptoactivos pueden ser objeto de elusión tributaria (delito contra la Hacienda Pública, si la cuota defraudada superara los 125.000 euros), pues en función del domicilio fiscal de quienes generen ganancias con su gestión/transacción, el hecho de tributar o no los activos (modelo 720) radicados fuera de España —ver la Ley 5/2022, de 9 de marzo[20]—, puede llevar a alcanzar la cifra que separa la mera infracción administrativa para convertirla en delito.

A lo anterior habrá que sumar los posibles delitos medioambientales —las CASP significativas deben revelar su consumo de energía e impacto ambiental y climático a la AEVM—, o delitos instrumentales vinculados, como puede ser el que se ocasione por usar identidades suplantadas al transaccionar criptos, sin olvidar su posible concurso con el delito de grupo criminal del Art. 570 ter CP, ya que, muchas veces su carácter transnacional, el uso de sociedades pantalla y paraísos fiscales, etc., añaden, a la realización de transacciones con criptos, la imposibilitación/obstaculización de identidades, de manera que se aplique el mismo régimen entre criptos y fiat, evitando el ingreso del producto delictivo en la economía legal.

[20] Jefatura del Estado, «Ley 5/2022, de 9 de marzo, por la que se modifican la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, y el texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado mediante Real Decreto Legislativo 5/2004, de 5 de marzo, en relación con las asimetrías híbridas», Pub. L. No. Ley 5/2022, § 1, BOE-A-2022-3712 28280 (2022), https://www.boe.es/eli/es/l/2022/03/09/5.

4. **ASPECTOS PROCESALES**

4.1. JURISDICCIÓN Y COMPETENCIA

Comoquiera que los criptoactivos se almacenan y transaccionan mediante sistemas electrónicos distribuidos por nodos que geográficamente pueden hallarse en el territorio de diferentes países, nos preguntamos cual es la jurisdicción competente para enjuiciar las infracciones que se cometan con/contra ellos, y qué Tribunal concreto lo hará.

En cuanto a lo primero, al abordar el enjuiciamiento de estos delitos tecnológicos, como normalmente se desconoce quién y desde dónde se ejecutan, dónde y cómo ocurren, y a través de qué espacios físicos, al desplegarse su acción en el espacio virtual, nos preguntamos qué país concreto puede enjuiciar una trama transnacional de esa clase.

En el caso de los fraudes/estafas —lo que es fácilmente extrapolable a los demás tipos de delitos con/contra criptos—, el considerando 20 de la EM D 2019/713[21], apelando a la eficacia, manifiesta que: "en general, lo más adecuado es que se conozca de una infracción en el marco del sistema penal del país en el que se ha cometido. Por consiguiente, cada Estado miembro debe establecer su jurisdicción para conocer de las infracciones cometidas en su territorio y de las infracciones cometidas por sus nacionales. Los Estados miembros pueden también establecer su jurisdicción para conocer de las infracciones que provoquen daños en su territorio".

De manera que, su Art. 12 expresa dos atribuciones jurisdiccionales principales —párrafo 1—:

- el país del territorio donde total o parcialmente se haya producido la defraudación (que, según el párrafo 2, comprende el territorio donde físicamente estaba el autor al cometer la infracción, independientemente de dónde estuviera el sistema informático que haya utilizado para llevarla a cabo) o

[21] «Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo», OJ L § (2019), http://data.europa.eu/eli/dir/2019/713/oj/spa.

- el de nacionalidad del autor; y tres potestativas -párrafo 3- ante la más que real contingencia de ignorar quién es el autor y dónde atacó:
- el país del territorio donde reside habitualmente el presunto autor,
- el de establecimiento de la empresa que haya obtenido provecho del delito o
- el de sus víctimas siempre que al menos residan habitualmente en él, de manera que este fuero alternativo basado en la producción del daño, por evidente, será el inicialmente más utilizado, al menos hasta que se descubra el presunto autor, en que operará el oportuno traslado de procedimiento.

Y ello en consonancia con la teoría de que las estafas se consuman (ver STS 61/2012, de 8 de febrero[22]) cuando, producto del ataque a una víctima concreta, se produce el desplazamiento/transferencia económica en su contra.

Si se trata de una defraudación tecnológica/maquinal, el delito se entendería consumado donde operase la transferencia, pero al no ejecutarse una traslación física del activo depredado, sino tan solo informática, que, precisamente suele pretender una disponibilidad universal por el acceso al mismo, normalmente, desde cualquier punto geográfico donde se pueda conectar a Internet, debemos buscar fueros alternativos jurisdiccionales más físicos, normalmente, a falta de conocer dónde radica el presunto defraudador: el de localización habitual/residencia de la víctima o el del lugar de manifestación del daño -la pérdida de la disponibilidad sobre el activo atacado-.

Caso de que hubiera varios países presuntamente competentes para enjuiciar la misma trama defraudatoria, el considerando 21

[22] Berdugo Gómez de la Torre, Juan Ramón, STS 61-2012, 8 de Febrero de 2012, ES:TS:2012:794 (Tribunal Supremo - Sala Segunda, de lo Penal 2012).

EM de la D 2019/713, apelando a las obligaciones establecidas en la Decisión Marco 2009/948/JAI[23] del Consejo y en la Decisión 2002/187/JAI[24] del Consejo, anima a las autoridades competentes a la posibilidad de establecer consultas directas con la ayuda de la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) para resolver ese conflicto jurisdiccional.

La atribución jurisdiccional en base al denominado criterio mosaico/fragmentación de la jurisdicción, esto es, el que lo establece en favor del lugar de manifestación del daño delictivo, tiene la ventaja de que a su vez permite la atribución para aplicar las medidas restrictivas tecnológicas como podría ser el caso del bloqueo/impedimento del acceso desde un territorio al ataque en línea desde otros, y alcanza a la persecución penal de las formas imperfectas de ejecución —tentativa, en los delitos de fraude con resultado— así como la de los delitos de riesgo por adelantamiento de la barrera punitiva.

En lo que hace a la competencia una vez ya dentro del Estado con jurisdicción, el problema, a falta de conocimiento de la concreta ubicación desde donde el presunto autor haya ejecutado el ataque, se repite.

Inicialmente, (Art. 14.2 LECRim[25]), será territorialmente competente para investigar este tipo de ataques delictivos, el Juzgado de Instrucción del lugar donde se hubiese cometido el delito.

Pero comoquiera que los cometidos a través de Internet tienen la potencialidad de causar efectos en muy plurales territorios

[23] Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales (s. f.).

[24] Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (s. f.).

[25] Ministerio de Gracia y Justicia, «Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.», BOE-A-1882-6036 § (1883), https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.

—de ahí las expresiones ciberespacio y mosaico—, la designación del concreto órgano judicial competente para instruir depende de que se aplique la:

- teoría de la acción -siendo competente el Juzgado territorial del lugar desde donde se inició el ataque-
- teoría del resultado/consumación —siendo competente el Juzgado de Instrucción donde se consume la acción, normalmente, el desplazamiento patrimonial, recepción del activo, su efectiva disposición, apoderamiento, ubicación de la cuenta receptora…— o
- cualquiera de ellos -teoría de la ubicuidad (Acuerdo PNJ TS 3/02/2005[26]), según la cual el delito se produce en todos los lugares en los que se hayan desarrollado las acciones del sujeto activo y pasivo: lugar del engaño, lugar de producción del perjuicio, lugar del desplazamiento patrimonial (A TS 31/01/2019:[27] 9/12/2020; 8/06/2021), que es la solución inicial adoptada por el Tribunal Supremo al resolver las cuestiones de competencia planteadas entre diversos Tribunales afectados por una misma trama defraudatoria, hasta que últimamente se ha venido corrigiendo, en función de la masividad o no del fraude, mediante la denominada teoría de la efectividad.

En efecto, como señala para estafas de inversión, en el caso del criptoactivo Bitcoin Rush el A TS 20.039/2022,[28] de 19/01/2022, la teoría de la ubicuidad sustituye a la de la consumación, haciendo competente al primer Juzgado que conoció del delito, en el caso de fraudes no masivos.

Porque en supuestos de fraudes masivos por Internet, se pre-

[26] Acuerdo PNJ TS 3/02/2005 (s. f.).
[27] A TS 31/01/2019 (s. f.).
[28] A TS 20.039/2022 (19 de enero de 2022).

fiere la teoría de la eficacia/facilidad en la investigación (A TS 16/01/2020;[29] 24/10/2019), de conformidad con Art. 22.5 Convenio Budapest de 2001 que aboga en favor del Juzgado que esté en mejores condiciones para ejercer la persecución del delito, de manera que la competencia debe ceder en favor del Juzgado del lugar donde operaba el atacante (Art. 15 LECrim) que es el que seguramente va a permitir el descubrimiento del mayor número de pruebas -especialmente el análisis forense de los dispositivos informáticos usados por aquel-.

4.2. DILIGENCIAS DE INVESTIGACIÓN

El Art. 13 D 2019/713 ordena a los Estados firmantes que para garantizar que las personas, unidades y servicios encargados de la investigación/persecución de las estafas tecnológicas actúen con eficacia, se garantice que puedan utilizar los mismos instrumentos de investigación que se emplean en la lucha contra la delincuencia organizada y los delitos graves, aplicándolos con la debida proporcionalidad.

De manera que, por remisión, acorde al Convenio ONU contra la delincuencia organizada transnacional de 15 de enero de 2000, hecho en Nueva York, cabe investigar tramas de fraudes/estafas usando —con la proporcionalidad que el Juez estime adecuada a las circunstancias del caso, y, en consecuencia, no para todo caso, y por supuesto en las llevadas a cabo por grupos/organizaciones criminales—, además de las clásicas diligencias procesales de averiguación, instrumentos tan restrictivos como:

- investigaciones conjuntas —equipos conjuntos de investigación—
- entregas vigiladas, de instrumentos/herramientas/programas para defraudar, así como de remesas económicas que ayuden a aflorar la identidad/ubicación real de los autores
- vigilancias tecnológicas y físicas

[29] A TS 16/01/2020 (24 de octubre de 2019).

- operaciones encubiertas de infiltración con agentes encubiertos
- testigos protegidos

Y figuras procesales como:

- la cooperación internacional, incluyendo además del intercambio de información policial, la asistencia judicial recíproca, con medidas como el traslado de denuncia al país mejor posicionado, la extradición o el traslado de personas condenadas para cumplir condenas y
- el embargo/incautación para asegurar futuros pronunciamientos de decomiso.

Además de lo anterior, la D 2019/713 únicamente añade especiales obligaciones de aportar información -ante las reticencias por razones reputacionales que suelen observarse- relacionada con las entidades intermediarias a través de las que se producen estas infracciones (Art. 13.2), que se convierten en exigencias de intercambio de información y denuncia (Art. 14) a través de un punto de contacto 24/7 nacional y de rápida —el precepto habla de 8 horas— respuesta informativa a las solicitudes urgentes que sirvan para hacer progresar las investigaciones.

4.3. ANÁLISIS FORENSE DE DISPOSITIVOS

Por otra parte, y dentro de las diligencias procesales de instrucción habituales, conviene resaltar la del análisis forense y con autorización judicial de los dispositivos tecnológicos usados presuntamente para delinquir, mediante la figura procesal del registro físico/remoto de los mismos (Art. 588 sexies LECrim). Es a través de esta figura que se pueden localizar evidencias y rastros tecnológicos que lleven a determinar que el usuario que las haya ejecutado sea el autor del ataque en cuestión.

En la búsqueda forense en ejecución del registro de los dispositivos tecnológicos, será donde pueden aparecer los rastros de ataques a sistemas y datos que hayan pretendido transacciones

económicas ajenas, las propias operaciones económicas a analizar, los instrumentos de pago inmaterial utilizados en sus acciones (i. e: monederos/billeteras virtuales (wallet) con sus claves públicas) sobre los que ver flujos económicos entre autor y víctima o entre autor y copartícipes, las herramientas/instrumentos/datos/programas informáticos diseñados o adaptados específicamente para defraudar, el acceso a cuentas bancarias, las consultas de datos de sus víctimas, etc., y hasta la clave privada o contraseñas usadas para operar.

Para hallarlo se podrán utilizar herramientas trazadoras de flujos entre wallets, tipo *chainanalysis,* y hacer consultas a las empresas de intercambio y gestión de monederos (Exchange y Wallet) para ir verificando no sólo las transacciones delictivas, sino a quién llegan y quién ayuda a su consecución.

La ejecución del registro estático de dispositivos tecnológicos con posibles evidencias del delito (Art. 588 sexies LECRim), exige que el Juez la autorice, tanto si es previsible su ocupación durante el registro domiciliario del sospechoso -párrafo a- en cuyo caso ha de indicarlo, como si se ocupan en espacios abiertos, no íntimos -párrafo b-, pues en ambos casos, "la simple incautación de cualquiera de los dispositivos ….., no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el Juez competente".

De manera que, al poder afectar al derecho del investigado a la privacidad de su información y datos personales y telecomunicaciones que se llevan a cabo y conservan en esos dispositivos, la Policía Judicial, en su labor auxiliar del Juez, no puede ir más allá de la incautación del continente, del dispositivo físico —protegiéndolo de accesos externos, por ejemplo mediante una bolsa Faraday, para evitar el borrado a distancia de su volátil contenido—, pero no puede analizarlo, sin permiso del Juez, que deberá motivar/justificar expresamente en su resolución por qué y en qué el acceso al contenido y a los posibles repositorios de datos relacionados sirven para descubrir el delito investigado.

El Juez en su autorización —párrafo c— "fijará los términos

y el alcance del registro" y con el añadido de las condiciones para mantener su integridad -que podría afectar a la fiabilidad del objeto de lo registrado cuando no se aplique la correcta cadena de custodia— y demás garantías para la preservación intacta de su contenido entre las que hay que posibilitar la presencia de la Defensa—, podrá ordenar realizar copias de su contenido para empezar a analizarlo.

El copiado de la información virtual contenida en el dispositivo a analizar, cuando se trasvasa bit a bit a un dispositivo almacenador de memoria copia —o fichero de imagen— se denomina clonación, y es una operación mecánica que realizan las máquinas clonadoras, bajo la observación del Letrado de la Administración de Justicia, que permite la comprobación tecnológica de su completud —mediante la verificación de su firma hash[30] — de manera que se constate que la información no sólo no ha sufrido alteraciones, sino que se conserva exactamente igual que la aprehendida en el dispositivo sospechoso, y así se garantiza que lo que se analice es lo mismo que lo que se ocupó.

La realización de las copias clonadas puede servir al técnico analista forense para trabajar con ellas en la libertad de que no importa que las incida durante su trabajo analítico, al guardarse el original precintado inalterable —en poder del LAJ—, y también al resto de partes personadas —Acusaciones y Defensas— para poder confeccionar y presentar sus periciales o contrapericiales de parte.

Si al analizar el contenido del dispositivo se descubre que los datos buscados están almacenados en sistema informático diferente o parte de él, con nueva solicitud de autorización al Juez, se podrá acceder a ellos si así lo permite el sistema del sospechoso o si están disponibles para este.

Se trataría de una ampliación del registro del dispositivo —párrafo c.3— por estar vinculada a lo investigado y derivarse de lo ya analizado, que puede autorizar el Juez desde el principio si sospecha que

[30] Cadena de caracteres alfanumérica obtenida a partir de la información clonada.

pueda ocurrir tal contingencia o que, caso de urgencia, puede ejecutar la Policía judicial o el Fiscal, informando inmediatamente a continuación —en todo caso en un plazo máximo de 24 horas- al Juez quien, en 72 horas, deberá confirmar o revocar la actuación, analizando las circunstancias de urgencia alegadas y la vinculación de lo ampliado con lo inicialmente aprehendido.

El análisis de la información y contenido de los dispositivos tecnológicos —computacionales como los logs de los ordenadores, o simples almacenadores de mera información, como un pen drive—, al incidir en derechos fundamentales del sospechoso como el de a su privacidad, protección de datos personales e incluso al secreto telecomunicativo, no puede llevarse a cabo sin autorización del Juez.

Sin embargo si intentar recabar esa habilitación judicial conllevara por sus circunstancias tal cantidad de tiempo que hiciera posible que se afectaran importantes derechos fundamentales —vida, integridad física, libertad…, pero no, como en el caso de las estafas, la simple defensa del patrimonio- de la víctima, la Policía judicial -párrafo c.4— podrá también proceder al análisis de la información incautada preliminarmente y para combatir la urgencia del derecho afectado —i. e: la geolocalización de un secuestro— sin autorización judicial, siempre que, inmediatamente después, y en el plazo máximo de 24 horas, por escrito motivado le cuenten al Juez competente las razones por las que tuvieron que conocer ese contenido y cómo y qué han injerido, de manera que, como en la urgencia regulada en su párrafo anterior, el Juez al final la convalide o revoque en un plazo máximo de 72 horas.

La norma —párrafo c.5— impone el deber de colaborar con los registros tecnológicos judiciales "bajo apercibimiento de incurrir en delito de desobediencia" a cualquier "persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria", siempre que no le suponga una carga desproporcionada, no se trate del propio investigado o encausado —que tiene derecho a no colaborar en la obtención de pruebas en su contra—, ni de

parientes cercanos o personas relacionadas con este por cuestiones de secreto profesional.

En lo que hace al registro remoto de dispositivos (Art. 588 septies LECrim), aplicable a la investigación de las estafas cometidas en el seno de una organización criminal —párrafo a.1.a— o a través de instrumentos, tecnologías o telecomunicaciones informáticas —párrafo a.1.e—, al suponer "la instalación de un software, que permita, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos", igualmente exige autorización judicial con el contenido que describe el párrafo a.2., pero con una autorización temporal de hasta un mes, prorrogable hasta un máximo de tres meses, dada la alta cantidad de información injerible y que se realiza en remoto.

Igualmente cabe el registro ampliado de la información si derivara en otro sistema informático —párrafo a.3— y se exige el deber de colaboración de terceros expertos neutrales en la ejecución del registro -párrafo b-.

4.4. EMBARGO/INCAUTACIÓN DE CRIPTOACTIVOS

Si al analizar el contenido de los dispositivos ocupados aparecieren activos económicos, o sus continentes virtuales —los monederos/billeteras wallet—, la Policía judicial debe proceder a incautarlos.[31]

Muy excepcionalmente, en fase inicial policial, cuando no hayan transcurrido más allá de 7-10 días desde realizada una transacción internacional producto de fraude superior a los 3.000 euros, la unidad policial investigadora, podrá remitir al Grupo 4 de Interpol Madrid correo electrónico en formato FLASH/URGENTE (ocinterpol@policia.es), solicitando de esta delegación española que Interpol bloquee policialmente de manera urgente la transacción trasnacional presuntamente delic-

[31] En virtud de lo dispuesto en los Arts. 282, 326.3 y 770.3 LECrim, así como específicamente en el Art. 11.1 g) de la LO 2/1986, de Fuerzas y Cuerpos de seguridad, ("recoger – asegurar y custodiar en todo caso- todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro"), así como por los Arts. 14 LO 1/1992, de 21 de febrero, de protección de la Seguridad Ciudadana y 28.e) RD 769/1987, de 19 de junio, de Policía Judicial.

tiva mediante lo que se ha denominado Protocolo I-GRIP (Interpol- Global Rapid Intervention of Payment), intervención rápida de pagos a escala mundial.

El indicado protocolo policial exige a la unidad solicitante que en el mail flash que dirija al Grupo 4 de Interpol Madrid indique:

- la actividad delictiva objeto de la solicitud (i. e: estafa) que debe ser transnacional
- un resumen del modus operandi empleado (i. e: estafa del CEO, phishing...)
- datos de las víctimas, existencia de denuncia y, en su caso, de procedimiento judicial
- fecha de comisión de los hechos -no deben haber transcurrido más allá de 7-10 días desde que haya operado-
- importe defraudado -debe ser superior a 3.000 euros-
- país de destino y solicitud de lo que se pretende (bloqueo de fondos)
- copia de la denuncia en español.

Una vez emitido el correo electrónico policial, el Grupo 4 de Interpol Madrid acusará recibo sugiriendo que la unidad remitente comunique su denuncia al Sepblanc (Unidad de Inteligencia Financiera española), al Juzgado competente para que solicite la correspondiente orden europea de investigación o comisión rogatoria internacional convalidando la petición de bloqueo/embargo de los fondos y al Banco afectado, con copia de la denuncia, para solicitar igualmente la retrocesión de la transferencia presuntamente delictiva.

La incautación/ocupación de efectos virtuales puede constituir:

- una medida cautelar asegurativa de futuros pronunciamientos penales o civiles, en nuestro caso, conforme al Art. 127 octies.1 CP, la consecuencia accesoria de su futuro decomiso, en lo que la norma llama aprehensión o embargo y posterior puesta en depósito judicial —

ante quien se convalidará o revocará la tal medida policial—, y

- un efecto del delito —de cara a su posible futura restitución (Art. 111 CP) en el campo de la responsabilidad civil—, que además podrá usarse como prueba -cuerpo del delito (Arts. 334-367 septies LECrim)- de su obtención fraudulenta, segunda razón por la que los Cuerpos Policiales deben ponerlos inmediatamente en depósito a disposición del Juez.

Comoquiera que los activos digitales no dejan de ser contenidos volátiles y alterables, fácilmente transaccionables, es aconsejable que, para incautarlos virtualmente de una forma más segura, se abra la billetera encontrada —para lo que hay que conocer la clave privada del sospechoso—, y se use la opción "enviar" o "transferir" remitiéndolo todo a una dirección pública preestablecida (la de la Policía o el Juzgado) donde llevar lo ocupado, de manera que, cuando se confirme la operación en la red, se habrá realizado su embargo a través de un monedero virtual público.

Las criptomonedas, activos inmateriales e intangibles, formalizan su custodia/almacenamiento —y la propia demostración de su existencia, título de propiedad y control real de los fondos/valor que encarnan— a través de billeteras/monederos virtuales, aplicaciones vinculadas a redes de registro distribuido (blockchain), que funcionan mediante el uso de claves públicas —direcciones para recibir monedas virtuales, que así quedan registradas en las cadenas de bloques— y privadas —que permiten transaccionar/traspasar/recibir y controlar personalmente las criptomonedas que se posean, estando asociadas a la dirección pública del usuario—.

De forma que cuando hablamos de la ubicación de los activos virtuales, y principalmente dentro de ellos, de las criptomone-

das, debemos entender que la información que las compone[32] se almacena en múltiples puntos del mundo, de manera sincrónica y descentralizadamente, en tantos nodos como forman la red de registro distribuido en que operan.

La información que compone el criptoactivo no se almacena en un ordenador que centralice todos los datos que la componen, sino que se guarda en los equipos interconectados a través del protocolo de Internet que forman la red[33] de ordenadores distribuidos mediante sus nodos —ordenador del usuario—, que a su vez validan las operaciones que realicen estos mediante un mecanismo de consenso que garantice que los bloques —y sus operaciones— se agregan correctamente y que todos sus nodos tienen la misma información.

Este almacenamiento descentralizado en red y la criptografía que acompaña sus transacciones hacen imposible la incautación del criptoactivo a través de entidades centralizadas como ocurre con los activos operados por la banca, por ejemplo.

El punto de conexión entre un concreto criptoactivo y su dueño/titular opera a través de esos monederos/billeteras virtuales que externamente se muestran a través de las claves públicas cuyo uso transaccional deja constancia en las redes blockchain, pero que internamente sólo puede manejar quien posea la clave privada que los accede, agregándola, de manera que se desconoce la identidad de quien transacciona, ya que lo único que se anota en la red blockchain es la dirección del remitente y el destinatario de la operación que, dado el anonimato de las claves privadas, se ignora quiénes son.

Los monederos/billeteras, que pueden estar custodiadas por terceras entidades prestadoras de servicios con criptoactivos que las gestionan —Wallet, que poseen la clave privada de uso— o simplemente ser autocustodiadas por su usuario —único cono-

[32] Datos digitales: datos informatizados que se representan mediante el uso de valores discretos (discontinuos) para incorporar información.

[33] La participación en una concreta red depende de que su acceso sea libre o abierto a cualquiera que quiera hacerlo —redes blockchain públicas— o restringido —redes privadas—.

cedor de su clave privada— utilizadas para transaccionar a través de esas cadenas de bloques pueden ser:

- Fríos (cold wallets): desconectados —por eso preferimos denominarlos unplugged— de la red, para dotarles de mayor seguridad —al conjurar ciberataques en línea—, de tipo hardware wallets (i. e.: Trezor), almacenados y conectables a la red a través de ordenador o teléfono móvil/celular mediante contenedores del tipo USBs, pen drives o lápices de memoria o códigos QR que dan acceso a las claves para ser usados, dado que las criptomonedas en realidad están almacenadas en la red, donde se custodian descentralizadamente y operan sus transacciones de manera que no se pueda acceder a ellas sin utilizar la clave privada, o bien mediante simple paper wallets, o anotaciones manuscritas de la clave privada —entre 12 y 24 caracteres sin relación entre sí— que después se usan igualmente a través de hardware/software wallets para conectar con su red blockchain y cerrar las oportunas transacciones.
- Calientes (hot wallets): conectados a Internet —plugged o enchufados— de tipo software wallets (i. e.: Metamask), aplicaciones informáticas almacenadas en línea, en webs o en la nube, accesibles desde cualquier parte del mundo a través de cualquier dispositivo: ordenador —software—, o teléfono móvil/celular -apps- permitiéndose transaccionar al abrirlas con sus claves privadas.

Con esas características técnicas, se entiende que, sin cooperación del poseedor de la clave privada, no es posible intervenir/bloquear/controlar el contenido de los billeteros fríos, aunque se pueda privar del continente —i. e: ocupando el pen drive clave— que necesiten para conectarse y transaccionarse, en cuyo caso, propiamente la incautación impide al investigado disfrutar de la posesión, pero no traslada al Estado la propiedad, control ni disfrute del criptoactivo contenido.

Y lo mismo que en las conectables, ocurre con los billeteros calientes salvo que se hackeen —i. e: mediante técnicas inmisivas, tipo puertas traseras o interceptativas, tipo man in the middle— ya que sin el conocimiento de su clave privada de uso será imposible conocer quién ejerce el control transaccional sobre los intangibles criptoactivos.

En la práctica, la dificultad para localizar e incautar criptoactivos sospechosos de ser producto del delito —al estar distribuidos por la red, haber numerosas redes de registro distribuido que se utilizan para operar de manera que rastrear sus operaciones sería costosísimo y desconocerse la clave privada de su usuario—, suele reducirse cuando aquel utiliza los servicios de las empresas servidoras de criptoactivos o intercambiadoras —Wallet/Exchange— obligadas por ley a colaborar con la Justicia.

Si el investigado presunto autor del ataque contrata con estas gestoras la custodia de sus criptos, improbable en el caso de delincuentes, de manera que aunque sean de su propiedad, quien conoce su clave privada para transaccionarlas es únicamente la proveedora, podrá el Juez ordenar a la empresa Wallet que: 1) las deposite en cuenta distinta —del Juzgado o externa temporal— hasta sentencia mediante la oportuna orden de embargo y con conocimiento judicial exclusivo de la nueva clave privada que las controla, o 2) tan sólo que las bloquee —prohibiendo a su custodiado/titular disponer/transaccionar con sus fondos—, continuando la Wallet en posesión de la clave privada, eso sí, sometida únicamente a las instrucciones sobre su destino que el Juez le indique —administración judicial— en función del resultado de las investigaciones y su posible enjuiciamiento.

El Auto judicial obligando a la empresa servidora de criptoactivos a la sujeción del intangible a disposición del resultado de la causa penal, debe ordenar el acuse de su ejecución donde se debe consignar el día, hora y saldo incautados, expresando igualmente qué concreta criptomoneda ha sido bloqueada, de cara a poder permitir el cálculo del importe indemnizatorio

actualizado en caso de fluctuar su valor en el tiempo.

Otro problema añadido derivado de la colaboración de las empresas prestadoras de servicios con criptomonedas radica en que si no tienen su sede física en territorio nacional, la ejecución de la orden de embargo se debe transmitir a través del oportuno instrumento de cooperación judicial internacional,[34] en el caso de las radicadas en el territorio de la Unión Europea en la forma consignada en el Título VII, resoluciones de embargo preventivo de bienes, Arts. 143-149 de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.[35]

Para que jurídicamente podamos hablar de embargo (Arts. 589-600 LECrim), debe ser el Juez quien convalide esa aprehensión virtual mediante cambio de claves privadas al criptoactivo, cuestión que podrá acordar bien expresamente mediante una resolución, previa o posterior a la ocupación digital, en la que podrá ser auxiliado por empresas servidoras de criptomonedas,[36] bien convalidando la ocupación policial, i. e.: por vía de resolución del recurso, motu propio o al resolver escrito de parte solicitándoselo.

En puridad, la búsqueda de criptoactivos comienza en el propio registro —allanamiento— domiciliario/personal del sospechoso, cuando se incauten/ocupen los dispositivos tecnológicos

---

[34] Para el territorio de la Unión Europea, a través del Reglamento (UE) 2018/1805 del Parlamento europeo y del Consejo, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo decomiso, y, para países extracomunitarios, la correspondiente comisión rogatoria internacional conforme disponga los Tratados de cooperación/asistencia jurídica penal bilaterales o multilaterales que mutuamente hayan suscrito, o caso extremo, conforme al principio de reciprocidad.

[35] Jefatura del Estado, «Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.», Pub. L. No. «BOE» núm. 282, de 21/11/2014, BOE-A-2014-12029 (2014), https://www.boe.es/buscar/act.php?id=BOE-A-2014-12029.

[36] Binance, i. e: previo requerimiento policial de la Guardia Civil, ha bloqueado, a disposición del Juzgado Central de Instrucción nº 4 de la Audiencia Nacional, el importe superior a los 1´77 millones de dólares resultante del balance positivo de las diferentes cuentas que los presuntos partícipes de Arbistar y Venus Capital -investigados por presunta estafa agravada (piramidal), falsedad en documento mercantil, organización criminal y blanqueo de capitales- tenían en esas plataformas de gestión de criptos.

—mejor si están conectados a red— con los que aquel esté relacionado: computadora, ordenador, portátil, laptop, tableta, teléfono móvil, celular…y las oportunas USB, memorias externas, pen drives, discos…. e incluso papeles cercanos donde, igual por suerte, podría encontrarse anotada la clave privada que abriese el monedero implicado en algún delito.

En el análisis técnico forense de su contenido, deben buscarse las transacciones/operaciones económicas y sus datos asociados que puedan constar, así como los monederos virtuales/wallet y las claves que los abren.

Para conectar operaciones económicas presuntamente delictivas con la participación criminal de los implicados en la trama defraudatoria, si la dinámica comisiva del delito se conoce por previas investigaciones operativas policiales, será interesante rastrear y agrupar las hechas a o desde una misma clave pública concreta, de manera que se pueda obtener información de a qué otras claves se dirige el activo y cuándo, lo que podrá servir, en combinación con otras informaciones y fechas conseguidas mediante otras diligencias —singularmente las aportadas por intervenciones telecomunicativas—, para conectar operaciones con sospechosos.

Igualmente será importante buscar las claves privadas de los monederos virtuales en las conversaciones/mensajes telecomunicativos sobre las propias operaciones económicas —i. e.: correos electrónicos—, archivos personales, documentos compartidos … o físicamente, incluso, en las cercanías del ordenador, escritorio, cajones, pen drives, papeles, pegatinas o notas manuscritas…del lugar donde vive o trabaja el sospechoso.

Aun así modernas tendencias de seguridad a veces impedirán el éxito de la búsqueda, pues proliferan los gestores de contraseñas compartidos —i. e.: Last Pass— o incluso de claves complementarias —que exigen agregar todas para acceder al activo—, cuando no el reparto de claves que pueden bloquear la cripto si se usan indebidamente (i. e: syrium, para ethereum, que permite contratos inteligentes de reparto de claves que necesitan de dos

o más personas para sacar dinero, firmar, unir su trozo de clave para que el contrato libere el bloqueo y envíe el dinero a tercero), por no hablar de los mixers, mezcladores/difuminadores usados para blanquear/lavar activos— que tratan de dificultar la trazabilidad de la información sobre la procedencia y el destino de las transacciones.

4.5. ASEGURAMIENTO/ALMACENAJE DE CRIPTOACTIVOS

Además, y comoquiera que muchos de los criptoactivos sufren todavía una alta fluctuación en su valor en función del paso del tiempo, es aconsejable —si nada opone el Juez por motivos de la investigación— proceder a su realización anticipada —a través del cauce que permite el Art. 367 quater d/e LECrim—, esto es, a su conversión en moneda de curso legal, en nuestro caso, en euros, para acabar físicamente custodiando estos en la Cuenta de Consignaciones y Depósitos Judiciales (en adelante CCDJ[37]), al menos en tanto en cuanto esta no opere con criptoactivos.

La realización o conversión en moneda fiat se podrá hacer externalizadamente a través de entidades privadas especializadas acreditadas —i. e.: Coindesk, que calcula la cotización media del cripto en los mercados— y que, restando su comisión, transferirán lo convertido en euros a la CCDJ, o mediante su transacción en pública subasta.

Una vez asegurado el cambio de custodio y poseedor de las claves del cripto incautado al sospechoso, evitando con ello posibles manipulaciones en remoto si se mantuviera la clave privada inicial, la custodia interina —hasta el resultado definitivo del juicio— la pueden llevar a cabo —pública— tanto el Juzgado, la Fiscalía como la Policía, bajo depósito judicial, pero también —privada— se le puede encomendar a una entidad custodia/Wallet, pagando por ese servicio.

Normalmente esa custodia bajo depósito judicial suele ser

[37] Ministerio de Justicia, «Real Decreto 467/2006, de 21 de abril, por el que se regulan los depósitos y consignaciones judiciales en metálico, de efectos o valores», Pub. L. No. Real Decreto 467/2006, § 1, BOE-A-2006-8345 18176 (2006), https://www.boe.es/eli/es/rd/2006/04/21/467.

pasiva y, en consecuencia, no se administran ni gestionan los criptos durante los a veces años de duración del pleito, o, como se ha indicado arriba, se realizan anticipadamente para custodiar euros en su lugar en la CCDJ.

Pero si se solicitara —por el investigado o alguna víctima— y el Juez lo acordara, dado el valor especulativo que estos activos virtuales pueden alcanzar como inversión al alza mediante el transcurso del tiempo, el Juez podrá acordar la intervención judicial especulativa de los mismos, normalmente encomendándosela (Art. 33.7 in fine CP) a alguna empresa gestora de carteras virtuales/Wallet.

Sobre la cuestión referente a quién sufre la pérdida por depreciación del valor de un criptoactivo cuando se compara lo que cotiza al momento de devolverlo o pagarlo y el momento en que se aprehendió por los investigadores —piénsese que normalmente hasta que la decisión judicial final es firme pasa mucho tiempo, a veces años, recursos incluidos—, las TS 998/2018[38], de 20 de junio, ha establecido que a efectos de responsabilidad civil, y al no tener un bitcoin consideración legal de dinero, se debe operar e indemnizar con la moneda legal con que se hizo la operación fraudulenta, euros, en el caso.

Estas cuestiones resarcitorias o no de la fluctuación monetaria de las criptomonedas se suelen resolver en la práctica solicitando al Juez una comparecencia de todas las partes para solicitarle la manera de hacerlo en función de sus intereses, de manera que, decidido el modo en función de las circunstancias de la investigación, el posible acuerdo de estas en presencia judicial vincule cuando se tenga que devolver —si absolución— o pagar —si condena— el producto del delito.

4.6. OBTENCIÓN DE LA CLAVE PRIVADA EN MONEDEROS VIRTUALES/WALLET

Hemos dicho que el conocimiento de la clave privada del monedero/billetero virtual wallet es crucial no sólo para acreditar la posesión,

[38] TS 998/2018 (20 de junio de 2018).

sino también la titularidad formal del propio criptoactivo,[39] -firma las transacciones y otorga acceso a los fondos- por lo que otro importante elemento de la investigación, será su obtención,[40] pues sin ella, se desconocerá la cantidad de activo encontrada, a la vez que hará que permanezca en poder del investigado.

La mejor manera de obtenerla será la colaboración, que podrá lograrse mediante las siguientes vías:

- información proveniente de cualquier instrumento de cooperación internacional policial o judicial (i. e.: intercambio espontáneo de información policial, o comisión rogatoria internacional)
- información proveniente de un testigo, que puede ser un transaccionador previo o incluso un ex gestor de carteras/monederos virtuales, que deberán aportar el dato de conformidad con lo recogido en el Art. 7 L. O. 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales,[41] que exige que su petición judicial/policial se fundamente motivadamente, que explique por qué su cesión es necesaria para la represión o prevención de infracciones penales —en nuestro caso ataques tecnológicos—, que se formule de manera concreta y específica -no masiva ni prospectiva-, y que se supriman los datos aportados —aquí la clave—- cuando dejen de ser necesarios para las averiguaciones que los motivaron.

---

[39] Las billeteras de criptomonedas no almacenan realmente los activos digitales. Lo que hacen es generar la información necesaria para poder utilizar criptomonedas. Son la condición técnica sin la cual no cabe acceder al activo, de manera que su posesión, equivale al título.

[40] Las claves pueden imprimirse en una hoja de papel, se puede acceder a ellas a través de un software de billetera para escritorio o estar almacenadas sin conexión a Internet en dispositivos de billetera hardware.

[41] Jefatura del Estado, «Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.», Pub. L. No. «BOE» núm. 126, de 27/05/2021, BOE-A-2021-8806 (2021), https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806.

- información (cuenta de mail; IP cercana; titular de la transacción o clave público- privada) proveniente de los proveedores de servicios de cambio (cajeros humanos, operadores de intercambio escrow[42] mediante aplicaciones) y de gestores de monederos virtuales wallet o Bancos, todos sujetos obligados por la Ley 10/2010 de prevención del blanqueo de capitales y financiación del terrorismo y por idéntico Art. 7 L. O. 7 /2021, o incluso de la propia Agencia Tributaria, si le consta.
- recabándola del propio sospechoso.[43] Comoquiera que tal acción ya es de por sí incriminatoria —conocerla es estar vinculado de alguna forma con el contenido del monedero—, su consecución voluntaria debe estar previamente precedida de la información en presencia de Abogado de su derecho a guardar silencio y a no colaborar aportando elementos incriminatorios en su contra. De manera que si, aun así, decide aportarla, se valorará en su caso como un acto de colaboración que podrá atenuar su futura responsabilidad penal ex Art. 21.7 CP[44] en relación con los párrafos 4 y 5 de ese precepto.

4.7. NOTIFICACIONES JUDICIALES A TRAVÉS DE NFTS. PREEMBARGOS

A veces ocurre que la operación/transacción fraudulenta delictiva —i. e.: el hackeo/robo de un monedero/billetera virtual— se conoce públicamente por haber operado en redes de registro

[42] Los pagos escrow son aquellos en los que el dinero permanece en custodia o depósito hasta que se completa correctamente la operación que origina el pago. En un servicio escrow, el pago no se realiza de forma directa, de una parte, a otra, sino a través de un tercero. Este agente externo custodia el dinero y lo entrega al destinatario cuando se hayan cumplido las condiciones previamente acordadas.

[43] Fue el caso de Mr X, responsable del mercado ilícito Silk Road, que pactó con la Fiscalía federal de San Francisco (EE UU) un acuerdo de entrega y confiscación estatal de los 70.000 bitcoins presunto producto de lo allí transaccionado, el segundo embargo más cuantioso hasta la fecha, por detrás del llevado a cabo en 2.022 por parte de la Policía sobre los presuntos autores del robo de bitcoins a la plataforma Bitfinex 3.600 a quienes se ocupó las claves privadas que custodiaban los fondos que lograron desviar de aquella. EE. UU. incauta US$ 3.600 millones en bitcoin robado en hackeo de Bitfinex (bloomberglinea.com)

[44] Jefatura del Estado, «Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.», Pub. L. No. «BOE» núm. 281, de 24/11/1995, BOE-A-1995-25444 (1996), https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

distribuidas o webs, pero se desconoce quién las ha llevado a cabo al haber maniobrado criptografiadamente.

Como además de la identidad del autor del delito es necesario que la investigación preserve también el producto económico derivado del mismo, para evitar el agotamiento delictivo que supondría transferirlo a tercero o consumirlo, se ha venido actuando judicialmente sobre su destino para impedirlo mediante notificaciones oficiales y públicas con NFTs[45] que suponen una especie de pre-embargo judicial del activo aunque sin sujeción real de su contenido, pero bajo apercibimiento de desobediencia, e ignorando sobre quién se hace, para tratar de evitar que terceras personas ayuden al ladrón a disfrutar de su botín.

Así, la resolución de la High Court del Condado de New York de 1/06/2022, en EE. UU., que permitió notificar mediante NFT a un hacker anónimo —que se había apoderado de activos virtuales por valor de 7´9 M $ mediante el hackeo de la Plataforma Exchange LCX— mediante una orden de restricción (de no recibir transacciones ni mover fondos por 1´2 M $).

A través de un token de servicio (NFT) emitió desde una dirección pública un aviso que se envió a la dirección de blockchain del destinatario de las criptos hackeadas insertando un hipervínculo/enlace a su orden de restricción judicial donde constaban sendas prohibiciones a quien quiera que fuera el hacker, de transmitir o recibir fondos bajo apercibimiento de incurrir en delito de desobediencia.

De manera parecida, la High Court de New York, en junio de 2022), mediante una orden de restricción temporal, prohibió la venta de la versión tokenizada del primer álbum del cantante Jay–Z y sus derechos de autor.

Por su parte, la High Court de Inglaterra y Gales, en un caso de estafa de suplantación (webs de corretaje clonadas) donde se defraudaron 2 millones de libras esterlinas por parte de "personas desconocidas", acordó que, al no disponerse de medio alter-

[45] Acrónimo de Non Fungible Token: certificado digital de autenticidad que mediante la tecnología blockchain se asocia a un único archivo digital.

nativo, se notificaran sus resoluciones judiciales y cautelares (embargo) por medio de NFTs con blockchain en el wallet del investigado.

Mediante este sistema pre cautelar, el órgano judicial puede enviar la orden oficial, verificando su trazabilidad, envío y depósito con éxito, desde su wallet público emisor y con un hash único, conminando a quien quiera que sea el autor, que le prohíbe disponer/transaccionar con su botín, a la vez que lo deja "marcado", pues aunque no puede verificar si el delincuente lo abre o no, advierte a terceros que pretendan interactuar con el wallet, de que no deben hacerlo bajo el riesgo también ellos, de verse envueltos en un delito.

En estas gestiones de "marcado" del producto delictivo, mediante la advertencia judicial a terceros de su relación con el delito, advirtiéndoles que ayudar a disponer de él constituiría cuanto menos una desobediencia, así como en la inclusión de activos escritos en redes blokchain en las correspondientes "listas negras" de Emisoras (donde se pueden censurar/congelar transacciones), es fundamental la colaboración de las empresas servidoras de criptoactivos, Exchange y Wallets.

En otro ámbito colaborativo entre lo público y lo privado en materia de investigación tecnológica de delitos, esta vez de propiedad intelectual, un Juez de Milán, en julio de 2022 ha ordenado a una prestadora de servicios tecnológicos, por un lado, bloquear webs "piratas" que disponían de productos intelectuales sin abonar contraprestaciones por derechos de autor mediante sus servicios DNS impidiendo a sus usuarios resolver (vincular con una IP concreta) los nombres de dominio afectados, y por otro, impedir a las plataformas DNS que dejen acceder a los bloqueados.

4.8. MEDIDAS RESTRICTIVAS TECNOLÓGICAS

Establece el Art. 13.2 LECRim que: "En la instrucción de delitos cometidos a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación, el Juzgado

podrá acordar, como primeras diligencias, de oficio o a instancia de parte, las medidas cautelares consistentes en la retirada provisional de contenidos ilícitos, en la interrupción provisional de los servicios que ofrezcan dichos contenidos o en el bloqueo provisional de unos y otros cuando radiquen en el extranjero".

En puridad se trata de unas "primeras diligencias", en cuyo Art. 13 LECrim se ubican porque, como señala su primer párrafo, tienen como finalidad "proteger a los ofendidos o perjudicados por el mismo, a sus familiares o a otras personas".

Se busca con ellas prevenir futuras víctimas y proteger a las potenciales actuales, retirando, cesando e impidiendo el canal técnico a través del cual se ejecuta el delito, impidiendo su efecto y continuación.

En definitiva, son medidas que hay que adoptar en las primeras fases de la investigación, más que para averiguar el hecho o su autor, para prevenir la continuidad de la actividad delictiva o sus efectos económicos y sociales; prevenir el agravamiento futuro; prevenir nuevas víctimas y ataques; reaccionar proactivamente frente a los efectos del delito; prevenir delitos futuros y proteger a las víctimas.

El Art. 13.2 LECrim les da la naturaleza de medidas cautelares de manera que no cabe duda de que se pueden/deben aplicar en la misma fase de instrucción —y no sólo como consecuencia de una condena en firme, tras la que, por supuesto, también son ejecutables— tan pronto aparezcan en la causa indicios de presunta actividad delictiva, valorando el Juez no sólo la apariencia delictiva y la vinculación con ella que tiene lo retirable/interrumpible/inaccesible (*fumus boni iuris*), sino igualmente el peligro que puede generar no hacerlo para terceras hipotéticas víctimas en el próximo futuro (*periculum in mora*).

En los delitos de estafas/falsificaciones tecnológicas se tratará de 1) retirar (y desindexar) contenidos, 2) interrumpir, cesar servicios o 3) impedir, bloquear el acceso a esos contenidos/servicios defraudatorios informáticos delictivos, que pueden ir desde los reclamos expandidos por Internet en webs, enlaces,

correos electrónicos, etcétera. hasta actuar sobre "los instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas" del Art. 249 CP o en su caso del Art. 400 CP, o retirar IPDEs inmateriales falsificados o auténticos pero receptados, una vez el LAJ lleve testimonio de ellos como prueba a la causa judicial que los investigue.

Comoquiera que el Art. 13 LECrim no explica cómo llevar a cabo la ejecución de esas medidas que pueden limitar derechos fundamentales como el de a la protección del dato personal, la privacidad e intimidad personal, el secreto telecomunicativo o la propia libertad de expresión y de información, aparte exigir autorización judicial, nos remitiremos al que fija el Reglamento 2022/2065 del Parlamento europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales (DSA), especialmente en cuanto al contenido de la "orden de actuación" (Art. 9.2 DSA).

La "orden de actuación" que regula ese precepto no indica el concreto contenido de la "actuación" que la orden del Juez debe encomendar a la empresa que preste el servicio digital que le auxilie técnicamente a retirar/interrumpir/bloquear, en la idea de que aquel vendrá diseñado/determinado por la norma nacional/comunitaria habilitante, dejando, en consecuencia, dentro de sus parámetros en la mayor libertad de determinación concreta a quien ordena, el Juez, que, en función de las necesidades y circunstancias concurrentes en su investigación penal concreta, optará por alguna o varias de entre las tres señaladas en el Art. 13.2 LECrim.

De esa manera, el precepto adjetivo procesal complementa la norma comunitaria.

El Art. 9.2 DSA exige que la "orden de actuación" describa detalladamente la intervención que se recaba, además de indicar el precepto legal nacional (aquí el Art. 13.2 LECrim) o

comunitario (que puede ser la propia DSA) que le habilita para emitir la orden, explicar por qué la información/contenido o servicio sobre la que actuar es ilícito, mencionando el precepto sustantivo nacional/comunitario que así lo conceptúe (i. e.: el precepto del Código Penal presuntamente infringido, Art. 249 ó 400 CP), su identificación como Autoridad judicial ordenante, la información técnica que permita al prestador identificar y localizar el contenido ilícito de que se trate, normalmente la URL exacta (i. e. https/www……..es, mailto/file/ftp/news…) o DNS sobre la que actuar, además de cualquier información adicional que ayude a localizarlo, información acerca de los mecanismos de recurso disponibles tanto para el prestador como para el destinatario del servicio que haya proporcionado el contenido y, en su caso, información sobre la Autoridad que debe recibir el reporte sobre el curso dado a la orden.

El dictado de la orden se rige por el principio de necesidad (Art. 8.2 b RSD), conforme al cual no debe el Juez exceder el ámbito de aplicación territorial más allá de lo necesario, ni afectar a más contenido que el adecuado a los hechos enjuiciados, el de legalidad, idoneidad, excepcionalidad, proporcionalidad y especialidad, conforme se definen en el Art. 588 bis a LECrim.

Y además debe observarse por parte del Juez el principio de progresividad en su posible aplicación, pues la retirada de contenidos es la medida menos restrictiva, mientras que la interrupción de servicios procede cuando se hace un uso delictivo del mismo de una manera no meramente circunstancial o episódica, y el bloqueo del acceso -de gran complejidad técnica- exige reiteración, proporcionalidad y efectividad, hasta el punto de que el precepto lo permite para cuando lo restringible "radique en el extranjero".

Complementa todo lo anterior en materia de auxilio inter-

nacional la normativa del Protocolo Adicional 2º del Convenio del Consejo de Europa sobre ciberdelincuencia de Budapest, al menos, dado que no ha entrado en vigor, como inspiración para las que deban desarrollarse fuera del territorio de la Unión Europea.[46]

4.8.1. Retirada de contenidos

Mediante la retirada (o desindexación) de datos y contenidos delictivos en las tecnologías informáticas se ordena extraer contenidos/datos parcial o eminentemente ilícitos, sin perjuicio de permitir la pervivencia de otros que sean inanes.

En nuestro caso, se trataría de la orden judicial de actuar pidiendo a la empresa prestadora del servicio informático donde se despliega, que técnicamente retire contenidos específicos (comprendidos en la URL oportuna) del producto informático (webs, blogs, foros, chats, redes, telecomunicaciones…servicios) que, en concreto, aparentemente esté sirviendo o ayudando a defraudar, del estilo de: los reclamos donde se expresa el engaño, el enlace donde se debe clicar o los adjuntos donde se despliega la defraudación, e igualmente los "datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas" tecnológicas del Art. 249 CP o los instrumentos técnicos para confeccionar las falsificaciones a que se refiere el Art. 400 CP.

De las tres medidas restrictivas tecnológicas es la menos intrusiva, dado que únicamente retira contenidos, los delictivos, pero ni necesariamente obliga a retirarlos todos, ni interrumpe el servicio donde se incorporaban.

De esa manera tan selectiva, además de cumplir con la obligación de respetar el principio de necesidad, se pueden acometer las retiradas de contenido delictivo que, afectando a una pluralidad de proveedores de contenido, discriminan en contra sola-

[46]A la espera de que algún día próximo se apruebe, primero, y ratifique, después, el proyecto de la ONU (redactado técnicamente en agosto 2024) de Convención Integral sobre la lucha contra la utilización de tecnologías de la información y las comunicaciones con fines delictivos, que trata la cooperación internacional en esa materia (Arts. 22 jurisdicción; 23-34 medidas procesales y 35-56 cooperación internacional).

mente de quien incorpora la ilicitud (i. e.: retirar de una web únicamente el trozo de contenido donde se ofrece el enlace delictivo que lleva a la descarga infectante de la manipulación informática defraudatoria, dejando el resto).

Sin embargo, la labor censurante no debe ser milimétrica, de manera que, en los casos de un presunto único creador, si el contenido de su producto informático es mayoritariamente lícito, no hay inconveniente en retirarlo todo.

Exigencias procesales obligan a que la retirada de contenidos delictivos se haga: en causa —expediente— penal abierta por hechos concretos, mediante Auto razonado por el Juez (único que puede restringir derechos fundamentales del sospechoso) donde se pondere y analice la relación que los principios de utilidad, legalidad, especialidad, necesidad idoneidad, excepcionalidad y proporcionalidad pueden tener en el caso concreto y considerando los indicios incriminatorios que se posean con la incidencia en los derechos fundamentales recogidos en los Arts. 18.1, 3 y 4 y 20 CE del investigado.

Igualmente, la causa debe corporeizar (i. e.: pantallazo, clonación) la virtualidad delictiva para conservarla bajo fe del LAJ como pieza de convicción de su existencia previa para los casos de tener que analizarla el forense tecnológico o, exhibirla como elemento/cuerpo del delito en un posible juicio oral posterior.

Además, el Juez deberá antes de emitir su orden -mandamiento- de actuación, verificar la existencia de lo denunciado, accediendo informáticamente al producto donde esté o comprobando por cualquier medio su existencia, de manera que, auxiliado técnicamente, pueda definir la URL a incidir, ordenando a continuación la retirada del contenido a la empresa prestadora de servicios donde se contenga.

E igualmente, como ordenará que no se comunique la restricción antes de ejecutarla para que no la aborte el autor, debe indicar a la empresa prestadora intermediaria que lo haga una vez ejecutado, de manera que, junto con el recurso que puede intentar la empresa —si discrepa—, le debe igualmente indicar (Art. 9.2.a.v

DSA) que contra la actuación, hecha por el Juez que sea -que también debe identificarse y señalar la causa penal concreta en que obra el Auto que lo ha ordenado-, cabrían los recursos de reforma y apelación en el plazo de tres/cinco días (Arts. 211 y 212 LECRim) a contar desde la notificación al afectado.

4.8.2.- Interrupción de servicios

También denominada "bloqueo" de la prestación o "suspensión" del servicio de intermediación, esta medida restrictiva impide el acceso a la información contenida en un servidor.

Se diferencia de la retirada en que la restricción tecnológica es mayor, pues se interviene y elimina la posibilidad de acceso a la totalidad del contenido del producto informático delictivo (i. e.: toda una web), que es el servicio que el prestador tecnológico incide.

Por ello debe reservarse para la interrupción de servicios informáticos donde su contenido sea entera o mayoritariamente delictivo, ya en cuanto a su contenido o por ser vehiculares de infracciones delictivas en sí mismo.[47]

A ellas aplican las formalidades que hemos indicado más arriba para la retirada de contenidos y las órdenes de actuación de la DSA.

4.8.3. Bloqueo de acceso

Tecnológicamente se trata de una medida restrictiva que, comprendiendo cualquiera de las dos anteriores o ambas —retirar o interrumpir—, aplica a los productos informáticos servidos desde fuera del espacio/espectro electromagnético soberano español, esto es, que no se provean desde nuestro territorio nacional, que es a lo que se refiere el Art. 13.2 LECrim cuando dice: "el bloqueo provisional de unos y otros cuando radiquen en el extranjero".

A la alternativa de acordar medidas de cooperación judicial internacional para que otro país las ejecute (órdenes de investigación, comisiones rogatorias), cabe impedir tecnológicamente desde España que el producto tecnológico delictivo acceda/entre al espectro electromagnético español, mediante esta medida técnica, que trata de com-

[47]En este sentido es interesante lo que indica la s TS 4ª en su sentencia 1.231/2022, de 3/10/2.022.

batir los efectos de reclamos delictivos servidos desde países "paraísos" informáticos.

Por su complejidad —incide en las URL o DNS, prohibiendo a los prestadores intermediarios tecnológicos que sirven desde España la distribución del producto informático delictivo en nuestro país—, debe ordenarse por el Juez únicamente con carácter excepcional y de manera temporal.

Pero comoquiera que la tecnología que sustenta Internet es tan "abierta" que hace, a la postre, imposible frenar la difusión de cualquier contenido ilícito, por su replicabilidad, la alternativa a esta costosa medida puede consistir en dirigir el mandamiento directamente a la empresa intermediaria extranjera que preste el contenido/servicio delictivo "sugiriéndole" la retirada voluntaria o la petición de que se lo traslade a la Autoridad competente en su país para hacerlo —lo que en la Unión Europea se canalizará a través del oportuno "coordinador de servicios digitales" (Arts. 49-51 DSA).

4.9. OTRAS MEDIDAS Y DECOMISO

Comoquiera que la delincuencia económica digital se expresa mediante la tecnología, ciertas actuaciones sobre esta pueden servir de prevención delictiva o como aseguramiento de una futura posible sanción contra un posible infractor económico tecnológico.

Consecuencia accesoria de todo delito patrimonial, mediante el decomiso (Art. 127.1 CP), el Juez acordará en sentencia la "pérdida de los efectos que de él provengan y de los bienes, medios o instrumentos con que se haya preparado o ejecutado, así como de las ganancias provenientes del delito, cualesquiera que sean las transformaciones que hubieren podido experimentar".

Se trata de una consecuencia accesoria, ínsita a la condena penal que necesita, obtenida tras un proceso judicial contradictorio y alejada de figuras como la actio in rem o acción directa contra bienes,[48] desligada de la sanción penal, que incauta/requisa/priva definitivamente al autor de un delito tanto de:

[48] Existentes en otros ordenamientos jurídicos, especialmente a través de la figura, muy útil en la lucha contra el crimen organizado, del denominado expediente de extinción de dominio.

- los efectos tecnológicos, instrumentos, herramientas, programas informáticos, dispositivos con los que haya cometido el delito —medios o instrumentos—, como
- las ganancias y activos económicos físicos o virtuales que haya obtenido como botín de sus ataques informáticos —efectos y ganancias—.

Ya hemos indicado más arriba que ambas vicisitudes deben asegurarse desde que conste en la causa el primer indicio del delito, mediante la medida provisional de su embargo cautelar, permitido para asegurar este pronunciamiento accesorio penal no sólo por la vía del Art. 127 octies.1 CP —que le deja iniciarlo incluso a la Policía auxiliar para poner inmediatamente lo aprehendido provisionalmente a disposición judicial—, sino también por la de la figura del embargo común regulado en los Arts. 589-600 LECrim.

Con el producto de la realización de lo incautado —más lo que se sepa fehacientemente transformado del mismo botín económico derivado de la defraudación— se debe indemnizar primero a las víctimas, y el sobrante se destinará al Estado, conforme dispone el Art. 127 octies 3 CP, cuando señala: "los bienes, instrumentos y ganancias decomisados por resolución firme, salvo que deban ser destinados al pago de indemnizaciones a las víctimas, serán adjudicados al Estado, que les dará el destino que se disponga legal o reglamentariamente", en un precepto especial y distinto del genérico Art. 126 CP que fija cuestión diferente, como es el orden en que se imputarán los pagos —el decomiso no lo es, sino que constituye una consecuencia, ope legis, para con los delitos que generan ganancias ilícitas, contrarrestando así el ánimo de lucro— que efectúe el penado y el responsable civil subsidiario.

FUENTES

A TS 31/01/2019 (s. f.).
A TS 16/01/2020 (24 de octubre de 2019).
A TS 20.039/2022 (19 de enero de 2022).
Acuerdo PNJ TS 3/02/2005 (s. f.).
Comisión Nacional del Mercado de Valores. Circular 1/2022, de

10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión, Pub. L. No. Circular 1/2022, § 1, BOE-A-2022-666 4106 (2022). https://www.boe.es/eli/es/cir/2022/01/10/1.

Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (s. f.).

Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales (s. f.).

Diario Oficial de la Unión Europea. Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (s. f.). https://www.boe.es/doue/2014/173/L00349-00496.pdf.

Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo, OJ L § (2019). http://data.europa.eu/eli/dir/2019/713/oj/spa.

Jefatura del Estado. Ley 5/2022, de 9 de marzo, por la que se modifican la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, y el texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado mediante Real Decreto Legislativo 5/2004, de 5 de marzo, en relación con las asimetrías híbridas, Pub. L. No. Ley 5/2022, § 1, BOE-A-2022-3712 28280 (2022). https://www.boe.es/eli/es/l/2022/03/09/5.

———. Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea., Pub. L. No. «BOE» núm. 282, de 21/11/2014, BOE-A-2014-12029 (2014). https://www.boe.es/buscar/act.

php?id=BOE-A-2014-12029.

———. Ley Orgánica 6/2021, de 28 de abril, complementaria de la Ley 6/2021, de 28 de abril, por la que se modifica la Ley 20/2011, de 21 de julio, del Registro Civil, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal., BOE-A-2021-6944 § (2021). https://www.boe.es/buscar/act.php?id=BOE-A-2021-6944.

———. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales., Pub. L. No. «BOE» núm. 126, de 27/05/2021, BOE-A-2021-8806 (2021). https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806.

———. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal., Pub. L. No. «BOE» núm. 281, de 24/11/1995, BOE-A-1995-25444 (1996). https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

———. Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso., BOE-A-2022-21800 § (2023). https://www.boe.es/buscar/act.php?id=BOE-A-2022-21800.

———. 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., BOE-A-2021-6872 § (2021). https://

www.boe.es/buscar/act.php?id=BOE-A-2021-6872.

Juan Ramón Berdugo Gómez de la Torre STS 61-2012, 8 de Febrero de 2012, ES:TS:2012:794 (Tribunal Supremo - Sala Segunda, de lo Penal 2012).

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo., Pub. L. No. BOE-A-2010-6737 (2010). https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737.

Ministerio de Gracia y Justicia. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal., BOE-A-1882-6036 § (1883). https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.

Ministerio de Justicia. Real Decreto 467/2006, de 21 de abril, por el que se regulan los depósitos y consignaciones judiciales en metálico, de efectos o valores, Pub. L. No. Real Decreto 467/2006, § 1, BOE-A-2006-8345 18176 (2006). https://www.boe.es/eli/es/rd/2006/04/21/467.

Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores., BOE-A-2015-11435 § (2015). https://www.boe.es/buscar/act.php?id=BOE-A-2015-11435.

«Reglamento (UE) 2023/ del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.o 1093/2010 y (UE) n.o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937», s. f.

TS 998/2018 (20 de junio de 2018).

Unión Europea. Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849., BOE.es-DOUE-L-2023-80807 § (2023). https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80807.