Adquisición de bitcoin mediante tarjetas prepagadas y «vouchers» no rastreables sin aportar datos personales: operativa, marco jurídico y consecuencias penales y administrativo-tributarias

NORBERTO MIRAS MARÍN

Profesor Contratado Doctor
Universidad de Murcia

RESUMEN

¿Se puede adquirir bitcoin con dinero en metálico sin dejar un rastro de datos personales? Adelantamos que sí. Y no es solo posible, sino que es sencillo. En este artículo se parte de algo al alcance de todos: la adquisición a cambio de efectivo de tarjetas y cupones prepagados no rastreables. Y se descompone su operativa de adquisición y su calificación en el marco jurídico español y europeo. A través de dichos cupones o vouchers se puede adquirir bitcoin, directamente en mercados descentralizados P2P, o a través del paso intermedio del voucher de bitcoin. Una vez adquiridos, se utilizará una cold wallet para almacenar sus claves privadas, exprimiendo al máximo el anonimato que nos puede dar el sistema. En una segunda parte del artículo, se estudian, desde una perspectiva doctrinal y jurisprudencial, las consecuencias jurídicas, tanto aspectos fiscales, como las obligaciones de identificación conforme a la Ley 10/2010 y los riesgos penales asociados.

Palabras clave: *bitcoin anonimato, compra de bitcoin con efectivo, cupones prepagados bitcoin, normativa bitcoin España, fiscalidad criptomonedas, blanqueo de capitales criptomonedas, Ley 10/2010, modelo 721 criptomonedas, MiCA, Travel Rule, criptoactivos legales.*

ABSTRACT

Can bitcoin be purchased with cash without leaving a trail of personal data? We anticipate that it is. And it's not only possible, it's simple. This article begins with something accessible to everyone: the acquisition of untraceable prepaid cards and vouchers. It breaks down their acquisition process and their classification within the Spanish and European legal framework. Through these coupons or vouchers, bitcoin can be acquired, directly in decentralized P2P markets, or through the intermediate step of the Bitcoin voucher. Once acquired, a cold wallet will be used to store their private keys, maximizing the anonymity the system can provide. The second part of the article studies, from a doctrinal, jurisprudential, and practical perspective, the legal consequences, including tax aspects, such as identification obligations under Law 10/2010 and the associated criminal risks.

Keywords: *buy bitcoin anonymously Spain, bitcoin prepaid voucher Spain, bitcoin tax Spain, AML crypto regulation Spain, bitcoin and Law 10/2010, MiCA compliance, Travel Rule crypto, bitcoin and money laundering, bitcoin legal status Spain.*

I. CONSIDERACIONES PREVIAS

La proliferación de criptomonedas, encabezadas por bitcoin, es una fuente constante de interrogantes en el plano jurídico y económico.

En particular, la posibilidad de adquirir bitcoin mediante *vouchers* prepagados y otros medios de pago no rastreables crea preocupación en ámbitos fiscales y penales debido a su anonimato. Las autoridades españolas y europeas han señalado expresamente que la economía digital y, en concreto, la operativa con criptoactivos, serán objeto de especial seguimiento. Esta atención responde al riesgo de blanqueo de capitales y evasión fiscal asociado a medios de pago opacos, así como a la falta de un marco normativo específico en etapas iniciales de la adopción de las criptodivisas –cosa que en la actualidad se ha solucionado con MiCA, las Directivas ATAD y el resto de legislación que regula el denominado ecosistema *cripto*–.

En este artículo se trata pormenorizadamente la cuestión de la compra de bitcoin utilizando medios de pago no rastreables –como cupones o tarjetas prepagadas adquiridas en efectivo–, analizando su operativa, el contexto tecnológico, el marco jurídico y las consecuencias en los órdenes penal, administrativo y tributario. Se seguirá una estructura sistemática: tras situar el contexto tecnológico y describir los medios de pago anónimos y el procedimiento paso a paso de adquisición, se estudiará el marco legal aplicable, la jurisprudencia relevante, así como aspectos de protección de datos y seguridad informática. Posteriormente, nos adentraremos en las tipologías de delitos e infracciones tributarias que pueden concurrir.

Asimismo, se considerará, como hemos señalado brevemente, el marco normativo europeo emergente y los desarrollos doctrinales recientes sobre la naturaleza jurídica de los criptoactivos. Con ello se pretende aportar una visión integral y fundamentada de esta cuestión, que se encuentra en un cruce de caminos entre la tecnología, el sector financiero y el derecho.

II. CONTEXTO TECNOLÓGICO

Comencemos describiendo brevemente la tecnología subyacente y la operativa típica de la adquisición de bitcoin, con énfasis en las modalidades que permiten cierto anonimato. Bitcoin es un activo digital descentralizado creado en 2008 por Satoshi Nakamoto (1), que

(1) El nacimiento de Bitcoin se sitúa el 31 de octubre de 2008, fecha en la que Satoshi Nakamoto publicó el *whitepaper* titulado «*Bitcoin: A Peer-to-Peer Electronic Cash System*» en la lista de correo de *cryptography* de *metzdowd.com*. Este documento sentó las bases teóricas y técnicas para el desarrollo de la primera criptomoneda descentralizada. Posteriormente, el 3 de enero de 2009, Nakamoto puso en marcha la red de Bitcoin al minar el bloque génesis, obteniendo una recompensa de 50 bitcoins.

opera sobre una red *blockchain* pública y distribuida. A diferencia del dinero de curso legal emitido por bancos centrales, bitcoin no está respaldado por ningún Estado ni depende de intermediarios financieros tradicionales para su funcionamiento. Las transacciones se validan mediante un protocolo criptográfico en una red *peer-to-peer*, quedando registradas de forma inmutable en la cadena de bloques. Esta tecnología permite transferencias directas de valor entre usuarios sin necesidad de una autoridad central, resolviendo el problema del doble gasto (2) mediante mecanismos de consenso descentralizados (3).

La forma convencional de adquirir bitcoin suele ser a través de plataformas de intercambio (*exchanges*) en línea, donde el usuario se registra y compra criptomoneda con moneda de curso legal mediante transferencias bancarias, tarjetas de crédito u otros medios de pago tradicionales. Tales plataformas suelen estar sujetas a regulaciones de prevención de blanqueo y requieren la identificación del cliente (procesos KYC, *Know Your Customer*) (4). Sin embargo, han surgido

---

Además, Satoshi protagonizó la primera transacción de la historia de Bitcoin al enviar 10 bitcoins a Hal Finney, un reconocido criptógrafo y desarrollador, el 12 de enero de 2009.

(2) Esta tecnología apuntaba en un primer momento como un medio de pago global con el que te «saltabas» en los pagos internacionales las cámaras de intercompesanción que te cobraban comisiones, así como cualquier otra comisión bancaria por gestión de pagos que te quisieran cobrar las entidades de crédito. Todo era ideología libertaria basada en trabajos del economista austriaco HAYEK. HAYEK, F. A., *La desnacionalización del dinero*, Unión Editorial, Madrid, 1983 (orig. 1976). [Consultado el 15 de octubre de 2025] en: https://archive.org/details/la-desnacionalizacion-del-dinero.

(3) Para garantizar la integridad del registro distribuido y evitar que un nodo malicioso modifique la cadena para adjudicarse fraudulentamente criptodivisas, el sistema *blockchain* recurre a un mecanismo de consenso distribuido que remite al denominado «problema de los generales bizantinos». Este dilema, formulado por Lamport, Shostak y Pease, plantea cómo alcanzar una decisión común entre múltiples participantes (generales) que no pueden confiar plenamente entre sí y cuya comunicación es indirecta y vulnerable a la traición. Aplicado al ámbito de las redes distribuidas, este problema refleja los desafíos de coordinar nodos que, sin conexión directa entre todos ellos y con la posibilidad de comportamiento malicioso, deben acordar la validez y secuencia de las transacciones. La blockchain aborda este reto mediante un sistema de votación basado en la potencia de cálculo (proof of work), de modo que la mayoría de la red determina qué versión de la cadena es la válida. Este mecanismo permite establecer una ordenación cronológica verificable de los bloques y asegura que cualquier intento de alteración maliciosa será rechazado por la red si no cuenta con la mayoría del poder computacional. LAMPORT, L.; SHOSTAK, R.; PEASE, M., «The Byzantine Generals Problem», *ACM Transactions on Programming Languages and Systems*, vol. 4, n.º 3, 1982, pp. 382-401.. [Consultado el 15 de octubre de 2025]. Disponible en: http://research.microsoft.com/en-us/um/people/lamport /pubs/byz.pdf.

(4) Existen «exchanges» sin KYC, que destacan por ofrecer accesibilidad y anonimato. *KuCoin* permite operar con más de 850 criptomonedas y ofrece una experiencia intuitiva sin necesidad de verificación, aunque limita las retiradas a 2 bitcoines diarios. *MEXC*, con más de 2800 activos cripográficos, brinda opciones de apalancamiento

métodos alternativos para comprar bitcoin de forma más anónima, sin vincular la transacción a una cuenta bancaria personal. Entre estos están los cajeros automáticos de bitcoin (*BATMs*) que aceptan efectivo, las plataformas de intercambio P2P (*peer-to-peer*) donde compradores y vendedores conciertan operaciones directas, y el objeto principal de nuestro estudio: la compra mediante *vouchers* prepagados y otros medios de pago no rastreables.

Un *voucher* es un término de origen inglés que, aunque no forma parte del diccionario de la Real Academia Española (RAE) en su forma original, sí aparece como «váucher» en algunas ediciones. Se trata de un documento que acredita el pago de un producto o servicio y que puede intercambiarse por el bien o servicio adquirido o bien cederse a otra persona para que esta última lo utilice (5).

En esencia, estos *vouchers* o cupones prepagados son códigos o tarjetas adquiribles a cambio de efectivo u otros medios (6), que luego pueden canjearse por bitcoin en determinados servicios o plataformas (7). Por ejemplo, en España existen empresas que distribuyen cupones canjeables por criptomonedas en miles de puntos de venta, incluidas grandes cadenas comerciales. El usuario compra un cupón de, digamos, cien euros, pagando en efectivo en un comercio minorista y obtiene un código. Posteriormente, ingresa ese código en la web o aplicación del proveedor del cupón para recibir el equivalente en bitcoin en su monedero digital. Este sistema separa la fase de pago –que ocurre de forma presencial y anónima en la tienda– de la fase de entrega de la criptomoneda en línea.

La motivación tras estas opciones es, en muchos casos, mantener el anonimato y evitar la trazabilidad bancaria de la transacción. Algunos usuarios simplemente valoran su anonimato financiero por razones legítimas. No obstante, la naturaleza opaca de estos métodos

---

y permite retiradas de hasta 30 bitcoines diarios sin KYC. Por su parte, *BingX* combina funciones como el *copy trading* y *staking*, con un límite diario de 50.000 euros. *Margex* se especializa en futuros con apalancamiento sin requerir verificación, mientras que *Best Wallet* es un *wallet* y un *exchange* descentralizado sin registro obligatorio ni límite fijo.

(5) Véase la explicación de la Real Academia de la Lengua. Real Academia Española, Diccionario Panhispánico del Español Jurídico, voz «váucher», s. f. [Consultado el 15 de octubre de 2025]. Disponible en: https://dpej.rae.es/lema/v%C3%A1ucher.

(6) Generalmente en establecimientos físicos, desde estancos a centros comerciales, pero también en G2A, que es un mercado digital internacional con sede en los Países Bajos y sucursales en Polonia y Hong Kong. Estas platagormas (G2A, Eneba, Kinguin) permiten a los vendedores vender claves de juegos digitales e incluso perfiles con las licencias dentro, licencias de software, tarjetas de regalo y otros productos digitales.

(7) También en estos mercados citados se pueden adquirir *vouchers* o cupones de bitcoines u otras criptomonedas o bien se puede acudir a mercados más especializados que las intercambian directamente.

también resulta atractiva para quienes buscan ocultar la procedencia de fondos ilícitos o evadir obligaciones fiscales, lo cual ha encendido alarmas en materia de prevención de delitos financieros (8).

Es importante señalar que bitcoin, en sí mismo, ofrece pseudoanonimato (9). Por tanto, la combinación de bitcoin con métodos de pago no rastreables multiplica la dificultad de seguir el rastro del dinero: en primer lugar, la entrada de fondos al ecosistema cripto se hace sin dejar registro identificable; en segundo lugar, la posterior circulación de los bitcoines puede diluirse entre múltiples direcciones digitales. Esta realidad tecnológica plantea un problema a las autoridades, que han venido desarrollando herramientas de *blockchain analysis* para rastrear transacciones sospechosas, pero que encuentran serios obstáculos cuando las cadenas se inician con conversión de dinero en efectivo o valores al portador en criptomonedas (10).

Así las cosas, desde el punto de vista operativo, la adquisición de bitcoin mediante cupones prepagados implica: 1.º la existencia de un proveedor o plataforma que ofrezca ese servicio –muchas veces regulada como plataforma de compraventa de criptomonedas–, 2.º una red de distribución de cupones o tarjetas –puntos de venta físicos donde el usuario paga sin revelar su identidad–y 3.º un procedimiento técnico de canje en el cual el usuario proporciona una dirección de *wallet* –monedero digital– para recibir sus bitcoines. A continuación, analizaremos con más detalle qué se entiende por medios de pago no rastreables y cómo funciona el procedimiento paso a paso.

---

(8) Véase un análisis de los patrones y riesgos en el uso de criptodivisas en: BOE, Anuario de Derecho, 2022. [Consultado el 15 de octubre de 2025]. Disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-2022-10042100446#:~: text=haz%20de%20direcciones%20bitcoin%20determinado, y%20Europeo%2C%20Modus%20Operandi%20y

(9) Las direcciones de la red no llevan nombre personal, aunque las transacciones son públicas y es posible «reconstruir» la identidad indirectamente a partir de herramientas como «chainanalysis», que conectan todos los datos referidos a las transacciones –emails, ip, otras operaciones–.

(10) Las herramientas de análisis *blockchain* (*blockchain analysis tools*) son aplicaciones especializadas que permiten rastrear, visualizar y analizar transacciones realizadas en redes *blockchain* públicas. Su funcionamiento se basa en algoritmos que analizan los datos públicos de la cadena de bloques –como la cronología, cuantía y relaciones entre transacciones–, a menudo complementados con fuentes externas *off-chain* (por ejemplo, registros de *exchanges*, filtraciones o redes sociales) para inferir la identidad de los usuarios o la naturaleza de los fondos. Plataformas como *Chainalysis, Elliptic* o *TRM Labs* permiten establecer vínculos entre nodos y detectar operativas sospechosas, siendo utilizadas por cuerpos policiales para reforzar el cumplimiento de las normativas contra el blanqueo de capitales y la evasión tributaria.

III. LOS MEDIOS DE PAGO NO RASTREABLES O «UNTRACEABLES»

Bajo la expresión «medios de pago no rastreables» nos referimos a instrumentos de pago cuyo uso no deja fácilmente un rastro nominativo en el sistema financiero formal, dificultando la identificación del pagador. Tradicionalmente, el efectivo –dinero en metálico– ha sido el medio no rastreable por excelencia: los billetes permiten transacciones anónimas. En el contexto digital actual surgen también medios electrónicos anónimos, tales como tarjetas prepago anónimas, cupones o *vouchers* prepagados, monederos electrónicos de prepago e incluso ciertas criptomonedas enfocadas en el anonimato –por ejemplo, *Monero* o *Zcash*– cuando se usan para adquirir bitcoin en intercambios descentralizados.

El uso de efectivo en transacciones de cierto valor se ha visto restringido por normativas antiblanqueo. En España, para combatir el fraude, la Ley 11/2021 –de medidas de prevención y lucha contra el fraude fiscal– redujo a mil euros el límite de pagos en efectivo en ciertas transacciones económicas entre empresarios o profesionales y particulares –antes situado en dos mil quinientos euros–. Aunque dicha limitación no impide al ciudadano común adquirir bienes con efectivo por encima de ese importe –salvo supuestos legales específicos–, sí refleja una política pública orientada a desalentar movimientos de capital opacos. A nivel de la Unión Europea, el Reglamento (UE) 2018/1672 regula el control de entrada y salida de efectivo en frontera, obligando a declarar cantidades de diez mil euros o superiores en efectivo o medios al portador al cruzar aduanas, y extendiendo el control a fondos no acompañados –enviados por mensajería, por ejemplo–, lo cual podría incluir instrumentos al portador distintos del efectivo tradicional (11). Estas medidas evidencian la preocupación por el carácter no rastreable del efectivo y medios similares.

Las tarjetas prepago –tipo monedero electrónico o *gift cards*– son instrumentos donde se carga un valor monetario que puede luego

(11) La normativa abarca no solamente el efectivo tradicional, sino también cheques al portador, valores negociables al portador y otros instrumentos financieros transferibles. Estos controles se extienden a envíos no acompañados realizados mediante servicios de mensajería o correspondencia postal, estableciendo un marco de supervisión integral que busca prevenir el uso de medios de pago no rastreables para actividades ilícitas. [Consultado el 15 de octubre de 2025]. Disponible en: https://sede.agenciatributaria.gob.es/Sede/normativa-criterios-interpretativos/normativa-aduanera/particulares/medios-pago.html#:~: text=Medios%20de%20pago%20, de%20efectivo%20de%20la

gastarse sin vinculación directa a la identidad del usuario, al menos dentro de ciertos límites (12). La normativa europea ha ido estrechando el cerco sobre el anonimato en estas tarjetas: la Quinta Directiva contra el Blanqueo (UE) 2018/843 redujo el umbral de anonimato de doscientos cincuenta euros a ciento cincuenta euros para las tarjetas prepago (13), de modo que por encima de ese importe –o acumulados ciento cincuenta euros mensuales– se requiere la identificación del titular. Además, la misma directiva facultó a los Estados para prohibir en su territorio el uso de tarjetas prepago anónimas emitidas en otros países (14). España transpuso estas medidas mediante el Real Decreto-ley 7/2021, imponiendo controles adicionales en la emisión y uso de dinero electrónico anónimo. Por tanto, las tarjetas monedero anónimas solo pueden usarse legalmente para pagos de pequeña cuantía; en importes mayores, deben ser nominativas.

Los cupones prepagados específicamente diseñados para la compra de criptomonedas operan con una lógica similar: permiten comprar con efectivo un valor que luego se canjeará por bitcoin. Desde la perspectiva legal, estos cupones pueden considerarse una forma de dinero electrónico o de vale al portador. La Ley 21/2011, de dinero

(12) Las normas contra el lavado de dinero restringen las transacciones en efectivo estableciendo umbrales para límites fijos de transacción y límites fijos de transacción en efectivo, basados en indicadores macroeconómicos como el PIB per cápita, el salario promedio y la escala de la economía sumergida. TANYUSHCHEVA, N., «Parámetros cuantitativos de la regulación antiblanqueo de capitales», *Análisis Financiero: Ciencia y Experiencia*, vol. 25, n.º 4, 2020. [Consultado el 15 de octubre de 2025]. Disponible en: https://doi.org/10.24891/df.25.4.416.

(13) Dentro de las principales modificaciones introducidas por la Quinta Directiva contra el Blanqueo de Capitales (Directiva (UE) 2018/843), que endureció significativamente los controles sobre instrumentos financieros prepago, tenemos la reducción del umbral de anonimato para tarjetas prepago desde los 250 euros establecidos en normativas anteriores hasta los 150 euros actuales. Esta medida forma parte de un paquete más amplio de reformas destinadas a cerrar las lagunas regulatorias que permitían el uso de estos instrumentos como vehículos para el blanqueo de capitales y la financiación del terrorismo. La directiva establece que, por encima de este umbral reducido, los emisores de tarjetas prepago deben establecer procedimientos de debida diligencia del cliente y verificación de identidad, eliminando así el carácter anónimo que anteriormente caracterizaba a estos productos financieros en rangos de valor más elevados. [Consultado el 15 de octubre de 2025]. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes-until-2027.html?fromSummary=23#:~: text=lex, a%20las%20UIF%20obtener

(14) La directiva introduce además una facultad discrecional significativa para los Estados miembros, permitiéndoles prohibir completamente en su territorio nacional el uso de tarjetas prepago anónimas que hayan sido emitidas por entidades financieras de otros países. Esta busca otorgar a las autoridades nacionales las herramientas necesarias para mantener la integridad de sus sistemas de prevención del blanqueo de capitales, independientemente del país de emisión del instrumento financiero.

electrónico, define éste como un valor monetario almacenado por medios electrónicos, aceptado como medio de pago por terceros distintos del emisor. Si bien los cupones de criptomoneda son canjeables únicamente en plataformas concretas, su funcionamiento guarda analogía con el dinero electrónico en cuanto almacenan un valor pagado previamente. La Ley 21/2011 y su normativa de desarrollo establecen obligaciones para los emisores de dinero electrónico, incluyendo registro y medidas contra el anonimato más allá de umbrales reducidos –por ejemplo, identificación obligatoria para recargas o pagos que superen los límites marcados en la normativa de prevención de blanqueo–.

En la práctica, los medios de pago no rastreables más empleados para acceder a bitcoin son: 1.º el efectivo –por vía de cajeros BTC o compra de cupones con cash–, 2.º las tarjetas de regalo o códigos de plataformas –algunas webs permiten comprar bitcoin entregando códigos de tarjetas regalo de grandes comercios, una modalidad P2P donde el origen del código es difícil de trazar–, y 3.º las tarjetas prepago de circuito abierto –tipo Visa o Mastercard, recargables– adquiridas anónimamente, que luego se usan en *exchanges*. Este último caso, sin embargo, está siendo cada vez más restringido por las políticas KYC de los *exchanges*: la mera posesión de una tarjeta no nominativa ya no garantiza anonimato si la plataforma cripto exige verificar la identidad al usarla.

Es relevante destacar que el concepto jurídico de «medios de pago» se ha actualizado. La Directiva (UE) 2019/713, relativa a la lucha contra el fraude con medios de pago distintos del efectivo, menciona expresamente instrumentos de pago electrónicos y los Estados miembros –incluido España, mediante LO 11/2022– han adaptado el Código Penal para incluir delitos de tenencia o tráfico ilícito de instrumentos de pago telemáticos. Si bien esa normativa se centra en la falsificación o uso fraudulento de tarjetas y similares, demuestra cómo la ley reconoce hoy una amplia gama de instrumentos monetarios no físicos. Incluso las criptomonedas han empezado a ser contempladas en definiciones legales: por ejemplo, la Directiva (UE) 2015/849 –4.ª Directiva AML– introdujo el término moneda virtual definiéndola como representación digital de valor no emitida por banco central, aceptada como medio de cambio por personas físicas o jurídicas. Más recientemente, la propuesta de Reglamento MiCA evita llamarlas «monedas» y opta por criptoactivos, subrayando que no tienen curso legal como la moneda de curso forzoso.

Por tanto, se consideran medios de pago no rastreables aquellos instrumentos que permiten «mover» un valor con escasa o nula información identificativa asociada. En el contexto de la adquisición de bitcoin, los protagonistas son el efectivo y las tarjetas y vales prepagados adquiridos con efectivo. Jurídicamente, el efectivo está sometido a limitaciones de uso y control en frontera, mientras que los vales y tarjetas prepagadas están sujetos a normativa de dinero electrónico y prevención de blanqueo que impone umbrales de anonimato bajos –ciento cincuenta euros– (15). Superados dichos umbrales, los emisores tienen la obligación legal de registrar la identidad del cliente y las operaciones, diluyendo así su carácter «no rastreable» (16).

IV. PROCEDIMIENTO DE ADQUISICIÓN DE BITCOIN A PARTIR DE METÁLICO COMPRANDO TARJETAS PREPAGADAS Y ADQUIRIR «VOUCHERS» O BITCOIN DIRECTAMENTE EN UN P2P O EN UN EXCHANGE SIN KYC

A continuación, estudiaremos con detalle el procedimiento típico para adquirir bitcoin con metálico mediante un *voucher* prepagado,

(15) La elección específica de ciento cincuenta euros como umbral no está documentada de manera explícita en cuanto a los cálculos precisos que llevaron a esa cifra exacta, pero el contexto normativo permite entender el razonamiento detrás de esta decisión. La Quinta Directiva contra el Blanqueo redujo el umbral desde los doscientos cincuenta euros anteriores hasta los ciento cincuenta euros actuales en respuesta directa a los ataques terroristas de París (noviembre 2015) y Bruselas (marzo 2016), donde supuestamente se utilizaron tarjetas prepago anónimas en la preparación de los ataques. El umbral de ciento cincuenta euros suponemos que representa un equilibrio calculado entre varios factores que la Comisión Europea consideró esenciales para el diseño de la normativa. Por un lado, buscaban mantener la utilidad de estos instrumentos para productos de dinero electrónico que presentan un bajo riesgo de blanqueo de capitales y financiación del terrorismo, permitiendo que las transacciones cotidianas de menor valor siguieran siendo posibles sin identificación y preservando así la funcionalidad legítima de estos medios de pago. Simultáneamente, intentaban reducir el riesgo de que los instrumentos prepago anónimos fueran utilizados para fines ilícitos, logrando una reducción del cuarenta por ciento respecto al umbral anterior de doscientos cincuenta euros. La normativa también estableció una gradación por tipo de transacción, fijando el umbral en cincuenta euros para operaciones *online* con tarjetas prepago, reconociendo el riesgo inherente a las transacciones remotas. Finalmente, la cifra refleja un intento de armonización con estándares internacionales de prevención del blanqueo, considerando las recomendaciones del Grupo de Acción Financiera Internacional y buscando coherencia con las mejores prácticas regulatorias a nivel global.

(16) Tienen la obligación, si están sometidos a una jurisdicción que la exige, habría que puntualizar.

ilustrando las etapas y señalando en qué puntos inciden las obligaciones legales.

1. **Adquisición inicial de la tarjeta prepago**

El proceso comienza con la compra física de tarjetas prepago, principalmente *Paysafecard* o *Neosurf*, en establecimientos autorizados, tales como estancos, gasolineras, supermercados o grandes superficies (17). Dicha adquisición puede realizarse directamente en efectivo, sin necesidad de aportar identificación personal, siempre que los importes sean inferiores a ciertos umbrales –habitualmente entre 50 euros y 100 euros, pero el límite es de 150 euros–. Estas tarjetas poseen códigos numéricos únicos no vinculados a cuentas bancarias ni registros personales, lo que preserva inicialmente el anonimato del comprador frente a terceros.

Desde una perspectiva doctrinal, este método de adquisición constituye una operativa técnica legítima, aunque conlleva ciertos riesgos derivados de su posible uso para ocultar fondos ilícitos, situación regulada bajo la doctrina penal de los «actos neutrales» (18). La jurisprudencia recalca la importancia de la responsabilidad

(17) También es posible su adquisición en la web, con el límite que hemos señalado en el anterior píe de página, en *markets* como G2A o Eneba, porque, simplemente, esa tarjeta prepago tiene un código y este puede adquirirse en internet. Eso sí, en ese caso no se puede utilizar metálico por razones obvias.

(18) El artículo 301 del Código Penal español establece la tipificación del delito de blanqueo de capitales, sancionando a quien adquiera, posea, utilice, convierta o transmita bienes a sabiendas de que proceden de una actividad delictiva. La norma extiende igualmente la punibilidad a quien realice cualquier acto destinado a ocultar el origen ilícito de dichos bienes o a ayudar a la persona que haya participado en la infracción a eludir las consecuencias legales de sus actos. La Sentencia de la Audiencia Provincial de Barcelona, Sección 3.ª, número 109/2020, constituye un pronunciamiento especialmente relevante en la delimitación de la responsabilidad penal en el contexto del blanqueo de capitales. Esta resolución aborda de manera específica el problema de cuándo una conducta aparentemente lícita puede adquirir relevancia penal si contribuye de forma consciente al delito cometido por un tercero. La jurisprudencia ha desarrollado progresivamente el concepto de actos «neutros», estableciendo que no resulta suficiente que una conducta sea objetivamente útil para la comisión del delito de blanqueo. El elemento determinante radica en la concurrencia del dolo, entendido como el conocimiento y la voluntad deliberada de colaborar en la actividad delictiva. Los denominados «actos neutrales», tales como la prestación de servicios profesionales o la realización de operaciones financieras, no constituyen conductas punibles cuando se ejecutan sin conocimiento del delito subyacente. Esta interpretación responde al principio fundamental de que la responsabilidad penal requiere necesariamente la concurrencia de elementos subjetivos que acrediten la intención delictiva. Sobre la doctrina jurisprudencial de los actos neutrales véase: SAP Barcelona, Secc. 3.ª, núm. 109/2020.

indirecta de los operadores en la prevención del blanqueo, aun cuando las tecnologías y procedimientos utilizados sean legales (19).

2. **Adquisición directa en *exchanges* o plataformas P2P**

Una alternativa técnica al uso de *vouchers* específicos consiste en utilizar directamente los códigos obtenidos de las tarjetas prepago –*Paysafecard*, *Neosurf*, *Flexepin*, entre otras– para comprar bitcoin en *exchanges* o plataformas peer-to-peer (P2P), como *LocalBitcoins*, *Paxful*, *Hodl*, o *exchanges* centralizados que acepten pagos mediante estos métodos (20). Esta operativa implica seleccionar un vendedor o plataforma que acepte la tarjeta prepaga, introducir directamente el código, y recibir posteriormente bitcoin en una dirección personal proporcionada por el comprador.

Desde el punto de vista doctrinal, esta opción presenta particularidades jurídicas relevantes, dado que elimina la intermediación de *vouchers* específicos y facilita la transferencia directa del activo virtual. Esta modalidad de compra debe considerarse a la luz del régimen jurídico establecido por la Ley 10/2010 y el reciente Reglamento MiCA, ya que los *exchanges* o las plataformas P2P pueden requerir distintos grados de identificación personal (*Know Your Customer* – KYC), especialmente cuando los importes superan ciertos límites operativos o regulatorios.

3. **Compra *online* de *vouchers***

El segundo paso consiste en utilizar la tarjeta adquirida (*Paysafecard* o *Neosurf*) para comprar un *voucher* específico canjeable directamente por bitcoin en plataformas especializadas como *Azteco*, *Kinguin* o *Coincards*. El usuario introduce el código numérico de la tarjeta prepago en la plataforma escogida, obteniendo así otro código

(19) En este sentido tenemos la SAP Asturias 37/2015, 6 de febrero de 2015. Sección Cuarta. Rollo: Recurso de Apelación 27/15. La Audiencia analizó el conflicto entre la empresa *Meetpays* S. L. y la entidad Caja Laboral Popular, que se negó a activar un TPV virtual para operaciones con bitcoines, alegando que no podía garantizar el cumplimiento de las medidas de diligencia debida exigidas por la Ley 10/2010. Aunque el contrato entre ambas partes era legal, el tribunal valoró que el uso de tecnologías como las criptomonedas –por su carácter anónimo y descentralizado– implica un riesgo elevado de blanqueo, lo que justifica una actitud especialmente cautelosa por parte de las entidades financieras.

(20) Por ejemplo, en los grandes *exchanges* como *Binance*, mediante plataformas intermedias.

específico que permite el acceso inmediato a una cantidad predeterminada de bitcoin. Este procedimiento se realiza generalmente sin que se requiera identificación personal en esta fase, lo que mantiene todavía cierto nivel de anonimato en la transacción (21).

4. **Canje e inscripción directamente en la *blockchain* principal *(on-chain)***

El tercer paso técnico consiste en el canje del *voucher* adquirido directamente por bitcoin en la *blockchain* principal (*on-chain*), prescindiendo así de redes intermedias. Para ello, el usuario debe acceder a la plataforma emisora del *voucher* –por ejemplo, Azteco.com– e introducir el código proporcionado junto con una dirección bitcoin generada previamente desde su *wallet* personal, preferentemente una cartera segura de tipo hardware (*Trezor, Ledger*) o una cartera no custodiada (*Electrum, Sparrow*). Una vez verificado el *voucher*, los fondos se envían directamente desde la plataforma a la dirección indicada, generando inmediatamente una transacción pública e irreversible registrada en la *blockchain* principal (22).

Desde la óptica doctrinal, este procedimiento elimina posibles vectores de exposición derivados del uso de redes secundarias, como la red *Lightning* (23). No obstante, incrementa la trazabilidad directa del movimiento, puesto que cada transacción queda registrada en la *blockchain* pública, visible para autoridades fiscales y entidades de

(21) Cabe señalar que algunas plataformas internacionalmente han ofrecido el canje de cupones sin identificación para importes bajos, aprovechando vacíos regulatorios o ubicaciones *off-shore*. No obstante, la tendencia normativa actual es cerrar esas brechas. Por ejemplo, Directiva (UE) 2018/843 incluyó a las plataformas de cambio de criptomonedas y proveedores de monederos custodios entre los «sujetos obligados» por la normativa antiblanqueo, lo que en España se tradujo en la obligación de registro ante el Banco de España y cumplimiento de KYC incluso para negocios de compraventa de cripto. En consecuencia, operadores serios de cupones como *Bitnovo* han debido utilizar procedimientos de identificación, contrariamente a la creencia de que esos cupones garantizan anonimato absoluto.

(22) Resulta especialmente interesante en esta materia el artículo de *ZenLedger*, «Cómo comprar bitcoin con tarjetas prepago en 5 pasos». [Consultado el 15 de octubre de 2025]. Disponible en: https://zenledger.io/es/blog/how-to-buy-bitcoin-with-prepaid-cards

(23) La red *lightning* es una solución de segunda capa construida sobre la *blockchain* de bitcoin que permite realizar transacciones rápidas y económicas. Fue diseñada para resolver los problemas de escalabilidad de bitcoin, como la lentitud y las comisiones altas de las transacciones en la red principal.

supervisión financiera (24). Esta característica se alinea con el marco de transparencia exigido por la regulación europea y española, particularmente en lo que se refiere a prevención del blanqueo de capitales, cumplimiento de obligaciones fiscales y modelos informativos –721, 172, 173–.

5. **Custodia segura y obligaciones posteriores**

Finalmente, tanto si el proceso se inicia en plataformas *exchanges*, mercados P2P o *vouchers* específicos, la etapa última y esencial para la custodia implica el envío directo de los fondos a una dirección bitcoin (*on-chain*). Esta transferencia implica una transacción irreversible que queda registrada permanentemente en la *blockchain*

(24) Ahora bien, el uso combinado de herramientas tecnológicas como las redes privadas virtuales (VPN) y el navegador Tor resulta útil para mejorar significativamente el anonimato del usuario durante la adquisición y el uso de criptomonedas. Sin embargo, estas medidas por sí solas no garantizan una protección absoluta frente a las técnicas avanzadas empleadas por empresas especializadas en análisis de *blockchain*, tales como *Chainalysis*, *Elliptic* o *TRM Labs*. Estas compañías aplican diversas metodologías complejas que exceden la mera identificación de direcciones IP. Entre ellas destacan: el análisis heurístico, que permite identificar patrones recurrentes en las transacciones para agrupar direcciones aparentemente no relacionadas; el análisis de agrupamiento o *clustering*, que facilita asociar diferentes direcciones utilizadas por un mismo individuo o entidad a través de patrones de comportamiento en la *blockchain*; y la colaboración activa con *exchanges* centralizados que aplican procedimientos KYC (*Know Your Customer*), permitiendo así la vinculación directa de la identidad del usuario con sus activos digitales. En este contexto, aunque la VPN ayuda a ocultar la dirección IP real del usuario al mostrar únicamente la dirección del servidor VPN y el navegador Tor proporciona múltiples capas de cifrado para evitar el rastreo inmediato, ambas herramientas presentan limitaciones. Por ejemplo, al utilizar *exchanges* centralizados que requieren la identificación personal (KYC), inevitablemente se crea un nexo identificable entre la identidad del usuario y sus criptomonedas. Asimismo, las empresas de análisis *blockchain* se apoyan en patrones transaccionales que trascienden la simple ocultación de la dirección IP, por lo que una única transacción no anónima puede comprometer toda la estrategia. Por lo tanto, una estrategia integral de anonimato frente a herramientas avanzadas como las utilizadas por *Chainalysis* y similares requiere el empleo simultáneo de múltiples capas. Entre las «soluciones» se encuentran la utilización exclusiva de plataformas descentralizadas (DEX) o servicios *peer-to-peer* (P2P) que no exigen KYC, el uso de técnicas avanzadas de mezcla de criptomonedas (*CoinJoin* o *mixers* o *tumblers* como *Samourai Wallet* o *Wasabi Wallet*), la adquisición inicial de criptomonedas a través de métodos menos rastreables (como *vouchers* físicos adquiridos en efectivo), así como el empleo sistemático de monederos jerárquicos (HD), generando nuevas direcciones para dificultar la agrupación y rastreo y también los novedosos *atomic swaps (*intercambios automáticos entre distintas *blockchains)* combinados con *zero-knowledge proofs (*protocolo criptográfico que permite a una persona demostrar que conoce cierta información sin revelar cuál es esa información*)*.

pública. El registro en la *blockchain* principal permite la trazabilidad si se disponen de las herramientas adecuadas.

En definitiva, este procedimiento técnico detallado no solo es viable desde un punto de vista operativo, sino que también cumple plenamente con las normativas en vigor, siempre que el usuario observe de manera estricta las obligaciones derivadas de la Ley 10/2010 de prevención del blanqueo de capitales y la normativa tributaria española aplicable.

Por tanto, el procedimiento técnico-operativo para adquirir bitcoin con medios no rastreables constaría de: compra anónima de un valor (cupón) con efectivo, interacción en línea para canjear ese valor por bitcoin y recepción de los bitcoines en un *wallet* del usuario. Cada una de estas etapas tiene implicaciones legales: desde el límite al anonimato en la fase de compra del cupón y las responsabilidades fiscales posteriores por tenencia o ganancia patrimonial. En los epígrafes siguientes profundizaremos en dichas implicaciones.

V. MARCO CIVIL Y MERCANTIL

Aunque este sea un asunto bastante manido, hay que reseñar que bitcoin carece de consideración de moneda de curso legal. El Tribunal Supremo, en su primera sentencia sobre criptomonedas (25), fue taxativo al afirmar que «el bitcoin no tiene la consideración legal de dinero». En dicha resolución penal, el Alto Tribunal caracterizó a bitcoin como un activo inmaterial de contraprestación o de intercambio, confirmando que no es moneda de curso forzoso ni dinero electrónico en los términos de la Ley 21/2011. Esta definición jurisprudencial se alinea con la postura del Banco Central Europeo y otras instituciones, que han señalado que las criptomonedas no son dinero desde una perspectiva legal, aunque voluntariamente puedan ser aceptadas como medio de pago entre partes. En esencia, para el derecho español vigente, bitcoin es un bien mueble inmaterial, susceptible de propiedad y de tráfico jurídico, pero no dinero ni valor mobiliario formal.

Esta calificación tiene consecuencias importantes: por ejemplo, la transmisión de bitcoines se rige supletoriamente por las normas civiles o mercantiles generales de transmisión de bienes. No siendo valores

(25) Miras Marín, N., «La determinación de la naturaleza jurídica del bitcoin a la luz de la reciente sentencia 326/2019 del Tribunal Supremo», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 51, 2019.

negociables ni instrumentos financieros regulados (26), la compraventa de bitcoines es un contrato atípico pero lícito, de objeto no prohibido (27). Asimismo, bitcoin está excluido del ámbito de protección de los sistemas financieros regulados (28).

A nivel europeo, el recientemente aprobado Reglamento (UE) 2023/1114 (MiCA), relativo a los mercados de criptoactivos, define y regula estos activos de manera uniforme. MiCA clasifica los criptoactivos en tres grandes categorías, *tokens* referenciados a activos, *tokens* de dinero electrónico –asimilables a *stablecoins*–, y otros criptoactivos– y establece requisitos de transparencia en su emisión, así como la obligación de autorización para los proveedores de servicios de criptoactivos (CASPs) (29). Aunque MiCA no convierte a los criptoactivos en moneda de curso legal ni instrumento financiero clásico, sí les reconoce explícitamente un estatus dentro del mercado interior, aportando certeza jurídica sobre su naturaleza: son representaciones digitales de valor o de derechos que pueden ser transferidas y almacenadas electrónicamente, pero que no han sido emitidas ni garantizadas por bancos centrales ni necesariamente vinculadas a moneda fiat. Por tanto, tras la plena aplicación de MiCA, la actividad de compraventa de bitcoin quedó sujeta a este marco, especialmente en lo que respecta a las obligaciones de las empresas que ofrezcan estos servicios –registro, capital mínimo, protección al cliente, por ejemplo (30)–.

---

(26) No encajan en las categorías de la Ley del Mercado de Valores.

(27) La sentencia del Tribunal Supremo confirmó la licitud de vender bitcoines, pero juzgaba una estafa en ese caso.

(28) No hay Fondo de Garantía de Depósitos que cubra su pérdida, por ejemplo, al no ser depósito bancario; ni está sujeto a supervisión de la CNMV salvo que se instrumente en productos financieros derivados.

(29) La normativa contiene diez categorías principales de servicios: custodia y administración de criptoactivos en nombre de clientes, gestión de plataformas de trading, intercambio de criptoactivos por fondos fiduciarios, intercambio entre diferentes criptoactivos, ejecución de órdenes, colocación de criptoactivos, recepción y transmisión de órdenes, asesoramiento sobre criptoactivos, gestión de carteras de criptoactivos, y provisión de servicios de transferencia. Esta cobertura abarca prácticamente todas las actividades comerciales significativas en el ecosistema de activos digitales. [Consultado el 15 de octubre de 2025]. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/european-crypto-assets-regulation-mica.html#:~: text=El%20Reglamento%20%20, proveedores%20de%20servicios%20de%20criptoactivos

(30) La Comisión Nacional del Mercado de Valores (CNMV) es la autoridad supervisora española documenta la implementación nacional del Reglamento MiCA y sus implicaciones específicas para el mercado español de criptoactivos. [Consultado el 15 de octubre de 2025]. Disponible en: https://www.cnmv.es/portal/mica/regulacion-criptoactivos?lang=es#:~: text=, y%20completa%20mediante%20libros%20blancos.

En suma, desde el punto de vista jurídico sustantivo, bitcoin es un objeto de propiedad privada, no dinero ni valor regulado, cuyo comercio cae en la esfera de la autonomía de la voluntad. Esta caracterización influye en el tratamiento fiscal: las operaciones con bitcoin no se benefician de exenciones o tratamientos monetarios salvo lo específicamente dispuesto en materia de IVA (vid infra) y su tenencia se equipara a la de otros bienes patrimoniales (31).

VI. REGULACIÓN DE PREVENCIÓN DE BLANQUEO DE CAPITALES Y OBLIGACIONES DE IDENTIFICACIÓN

El eje central del marco jurídico que incide en la compra de bitcoin con medios opacos es la normativa de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBC/FT). En España, la Ley 10/2010, de 28 de abril, junto con su Reglamento, establecen las medidas de diligencia debida, control interno y comunicación de operaciones sospechosas para los llamados sujetos obligados –entidades financieras, notarios, casinos, profesionales, entre otros–. Hasta hace pocos años, las actividades de intercambio de criptomonedas no figuraban entre dichos sujetos obligados, creando un vacío normativo (32). Esto cambió a raíz de la adaptación del marco europeo: la Directiva (UE) 2018/843 (5.ª Directiva AML) amplió el alcance a los «proveedores de servicios de cambio entre monedas virtuales y moneda fiduciaria» y a los proveedores de monederos de custodia. España transpuso esta directiva mediante el Real Decreto-ley 7/2021, de 27 de abril, que modificó la Ley 10/2010, incluyendo expresamente a dichos operadores cripto como sujetos obligados. Consecuentemente, desde abril de 2021, cualquier empresa o persona física que ofrezca en España servicios de cambio de criptomonedas por dinero tradicional, o que

(31) Wang ha propuesto la adopción de un régimen simplificado para la tributación de las criptomonedas, basado en su consideración como una clase específica de activos digitales con reglas propias y estandarizadas, que eviten las fricciones interpretativas del sistema actual. Wang, J., «A Simplified Tax Regime for Taxing Cryptocurrencies», *Intertax*, vol. 53, n.º 3, 2025.

(32) En 2015 las autoridades españolas reconocían expresamente que las operaciones de compraventa de bitcoines no se encontraban contempladas dentro del catálogo de actividades sujetas a las obligaciones de prevención del blanqueo de capitales establecidas en el artículo 2 de la Ley 10/2010, de 28 de abril. Esta laguna regulatoria permitía que los intercambios de criptomonedas operaran sin estar sometidos a los controles, procedimientos de diligencia debida y obligaciones de información de operaciones sospechosas que sí aplicaban a las entidades financieras tradicionales y otros sujetos obligados.

custodie criptodivisas de clientes, debe cumplir las obligaciones PBC/FT (33).

Además, el RDL 7/2021 impuso la creación de un Registro de Proveedores de Servicios de Criptoactivos en el Banco de España, en el que deben inscribirse tales entidades para poder operar legalmente. Esto fue implementado y actualmente decenas de plataformas han sido registradas tras acreditar procedimientos de prevención de blanqueo. De hecho, se otorgó un plazo –9 meses desde la norma– para que los *exchanges* se apuntasen en dicho registro so pena de no poder continuar su actividad legalmente. Junto a ello, la Ley 10/2010 exige que tales compañías designen un representante ante el SEPBLAC y apliquen todas las medidas de diligencia debida como cualquier entidad financiera.

El marco normativo ha avanzado hacia la inclusión explícita de los proveedores de servicios de criptomonedas como sujetos obligados en la lucha contra el blanqueo. López Martínez expone que, desde 2021, tanto los intercambios cripto-fiduciarios como los custodios de monederos están legalmente obligados a aplicar medidas de diligencia debida, lo que implica una «ruptura del modelo inicial de anonimato absoluto que se atribuía a los criptoactivos» (34). Esta evolución normativa permite interpretar que los *vouchers* prepagados para adquirir bitcoin podrían estar sometidos a regulación indirecta si se conectan con plataformas obligadas.

Esta normativa implica que los proveedores de cupones prepagados para bitcoin, en la medida en que son intermediarios de cambio, son sujetos obligados dentro del marco de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo. Por tanto, están compelidos por ley a identificar a sus clientes cuando concurran las circunstancias

(33) Es curioso que se siga omitiendo otro tipo de criptoactivos que pueden ser depósito de valor como los NFT. Fetsyak Senkiv ha advertido sobre el uso de tokens no fungibles (NFT) como vectores tecnológicos para el blanqueo de capitales y la financiación del terrorismo. En su estudio publicado en REDUR, destaca que el pseudoanonimato de estos activos, unido a su creciente popularidad en mercados opacos, genera nuevos escenarios de riesgo que escapan parcialmente al radar de la legislación vigente, más centrada en criptomonedas tradicionales. Fetsyak Senkiv, I., «Consideraciones sobre la prevención del blanqueo de capitales y financiación del terrorismo mediante los tokens no fungibles (NFT)», *Revista Electrónica de Derecho de la Universidad de La Rioja* (REDUR), n.º 20, 2022, pp. 91-103.

(34) López Martínez, M., Situación de la regulación de la prevención del blanqueo de capitales y de la financiación del terrorismo en el marco de los criptoactivos, *Instituto de Estudios Financieros*, 2023. [Consultado el 15 de octubre de 2025]. Disponible en: https://www.iefweb.org/publicacio_odf/situacion-de-la-regulacion-de-la-prevencion-del-blanqueo-de-capitales-y-de-la-financiacion-del-terrorismo-en-el-marco-de-los-criptoactivos/

establecidas –lo cual abarca prácticamente cualquier canje de cupón, salvo quizá importes ínfimos, ya que la normativa antiblanqueo exige identificación no solo en relaciones de negocio continuadas sino también en operaciones ocasionales por importe superior a 1.000 euros en efectivo, umbral ampliamente superado en la mayoría de compras de cripto relevantes, e incluso inferiores si hay indicios de fraccionamiento– (35).

Otro elemento relevante es la Directiva (UE) 2018/1673, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal. Esta directiva –transpuesta tardíamente por España a través de la Ley Orgánica 6/2021, de 28 de abril– no impone obligaciones a particulares directamente, pero armoniza la tipificación penal del blanqueo. Incluye, entre otras cosas, que los Estados deben reconocer como delitos precedentes del blanqueo a los delitos fiscales –directos e indirectos– (36), y que deben sancionar el *autoblanqueo* –la directiva insta a castigar también el blanqueo realizado por quien generó el dinero ilícito, figura que España ya contemplaba pero que se reforzó–. La Ley Orgánica 6/2021, de 28 de abril, complementaria al RDL 7/2021, en la reforma del Código Penal al modificar los artículos 301 y 302 CP introduciendo, entre otras novedades, nuevas circunstancias agravantes para el delito de blanqueo de capitales. En concreto, se elevan las penas si: (a) el dinero blanqueado proviene de determinados delitos especialmente graves o, (b) si el autor del blanqueo es sujeto obligado por la normativa de prevención de blanqueo. Esta segunda agravante resulta directamente aplicable a entidades que manejan criptomonedas: si, por ejemplo, directivos de una plataforma de compraventa de bitcoines facilitan dolosamente operaciones de lavado, al ser sujetos obligados –por Ley 10/2010– enfrentarán penas agravadas –prisión de 3 años y 3 meses hasta 6 años, según la reforma–. Es una advertencia del legislador a las empresas que tratan criptoactivos y que no cumplan y no sigan las directrices anti-blanqueo de que recibirán un castigo severo.

---

(35) Así se explica, por ejemplo, la política de Bitnovo de requerir verificación al canjear cupones: el proveedor se blinda ante la ley. Cualquier proveedor que anunciase anonimato total estaría navegando en la ilegalidad o aprovechando resquicios (por ejemplo, alegar que la obligación formal de KYC es a partir de mil euros en una sola operación, lo cual podría permitir canjes anónimos menos de mil euros; pero, aun así, la vigilancia de operaciones fraccionadas lo desaconseja, pues la Ley 10/2010 artículo 2.2 obliga a sumar operaciones fragmentadas). [Consultado el 15 de octubre de 2025]. Disponible en: https://www.bitnovo.com/comprar/efectivo/#:~: text=Reg%C3%ADstrate%20si%20eres%20nuevo

(36) [Consultado el 15 de octubre de 2025]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81801#:~: text=

En paralelo, la Unión Europea continuó ampliando el marco normativo con el Reglamento (UE) 2023/1113, conocido como Reglamento de Transferencia de Fondos, que extiende la «travel rule» a las transferencias de criptoactivos. A partir de finales de 2024, los proveedores de servicios sobre criptoactivos deben acompañar las transferencias de criptoactivos con información sobre el ordenante y el beneficiario, para asegurar la trazabilidad e identificar posibles operaciones sospechosas (37). Esto significa que incluso los movimientos entre *exchanges* o entre un *exchange* y un *wallet* privado no quedarán totalmente fuera del radar. Así, cuando un usuario envíe bitcoines desde un *exchange* regulado a una *wallet*, el *exchange* deberá registrar a qué cliente pertenecía esa *wallet* y lo mismo al recibir. También con el Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, aplicable a partir del 10 de julio de 2027, se amplía el marco. Este instrumento normativo establece un régimen considerablemente más estricto para los criptoactivos, incluyendo la obligación de que los empleados de entidades obligadas, incluidos agentes y distribuidores, participen en cursos especiales de formación continua específicos para reconocer operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo (38).

---

(37) Aunque trataremos con profusión estos asuntos en el epígrafe correspondiente al delito de blanqueo de capitales debemos adelantar que el reglamento introduce la obligación para los proveedores de servicios de criptoactivos de acompañar todas las transferencias con información completa sobre el ordenante y el beneficiario, incluyendo datos de identificación, direcciones y números de cuenta o cartera digital. La normativa elimina prácticamente los umbrales mínimos que anteriormente permitían transferencias anónimas de pequeñas cantidades, estableciendo que incluso las operaciones de valor reducido deben incluir información de trazabilidad. [Consultado el 15 de octubre de 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/es/LSU/?uri=oj: JOL_2023_150_R_0001#:~:text=Garantiza%20la%20trazabilidad%20de%20las, Aplica%20normas

(38) Aunque no se queda en eso en el ámbito de los criptoactivos, el Reglamento (UE) 2024/1624 (AML) integra plenamente a los crypto-asset service providers (CASP) como sujetos obligados en la prevención del blanqueo y la financiación del terrorismo; prohíbe la tenencia y apertura de cuentas cripto anónimas y el uso de mecanismos de anonimización (incluidas monedas con funciones de anonimización) por entidades financieras y CASP; exige KYC en operaciones ocasionales de más de mil euros; obliga a informar de transferencias con carteras autocustodiadas (self-hosted wallets), sin prohibirlas; establece medidas reforzadas para las operaciones transfronterizas entre CASP; y se coordina con la «travel rule» del Reglamento (UE) 2023/1113.

VII. CONSECUENCIAS FISCALES: TRIBUTACIÓN Y OBLIGACIONES INFORMATIVAS

Desde el punto de vista tributario, la adquisición de bitcoin con *vouchers* prepagados tiene implicaciones en impuestos y declaraciones. Podemos distinguir en: imposición indirecta (IVA) (39), imposición directa –IRPF e Impuesto sobre el Patrimonio– y obligaciones informativas especiales sobre criptoactivos.

Respecto al IVA, en la UE, las operaciones de cambio de moneda tradicional por criptomoneda –y viceversa– están exentas de IVA al equipararse a prestaciones financieras relativas a medios de pago. Esta doctrina emana de la sentencia del TJUE de 22 de octubre de 2015 (asunto Hedqvist), que interpretó que el bitcoin, careciendo de otro fin que el de ser medio de pago entre particulares, debía recibir el mismo tratamiento fiscal que las divisas tradicionales a efectos de IVA (40). España asumió dicho criterio: la Dirección General de Tributos ha confirmado que la compra-venta de criptomonedas contra euros está exenta de IVA por aplicación del artículo 20. Uno.18.º de la Ley del IVA –que exime las operaciones relativas a «divisas, billetes de banco y monedas que sean medio legal de pago», interpretación extensiva por mandato del TJUE– (41). Por tanto, cuando un usuario adquiere bitcoin a través de un cupón, no se devenga IVA sobre el valor del bitcoin en sí. Únicamente, si el intermediario cobra una comisión explícita, cabría analizar si esa comisión forma parte de la operación exenta –comisión de cambio de divisas, exenta también– o si es un servicio aparte; la postura común es considerarla parte de la operación financiera exenta. En la práctica, esto significa que el precio que paga

(39) Tal como ha señalado Capaccioli, el tratamiento del IVA respecto al bitcoin como medio de pago generó un intenso debate doctrinal, dado que su naturaleza jurídica escapa a las categorías tradicionales del Derecho tributario, oscilando entre la asimilación a moneda y la calificación como activo financiero, con efectos dispares en la imposición indirecta. Capaccioli, S., «VAT & BITCOIN», EC Tax Review, vol. 23, n.º 6, 2014.

(40) El tribunal fundamentó su razonamiento en que Bitcoin, al carecer de finalidad distinta a la de servir como medio de pago entre particulares, cumple las características esenciales de un instrumento monetario y, por tanto, debe beneficiarse de la misma exención aplicable a las operaciones de cambio de divisas bajo el artículo 135.1.e) de la Directiva 2006/112/CE del IVA. [Consultado el 15 de octubre de 2025]. Disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-2022-10042100446#:~: text=distinta%20de%20la%20de%20ser, relativa%20a%20la%20protec%02ci%C3%B3n%20penal.

(41) A mayor abundamiento en el régimen tributario: Miras Marín, N., «El régimen jurídico-tributario del bitcóin», Estudios financieros. Revista de contabilidad y tributación: Comentarios, casos prácticos, n.º 406, 2017, pp. 101-136.

el usuario –por ejemplo, 200 euros por el cupón– no lleva IVA, ni se podrá deducir nada tampoco (42).

En sede del Impuesto sobre la Renta de las Personas Físicas, la mera adquisición de bitcoin no es un hecho imponible en IRPF (no es un ingreso ni una ganancia en ese momento, sino una mera trasformación de un activo –dinero– en otro –criptomoneda– al mismo valor). Sin embargo, las posteriores variaciones patrimoniales que se produzcan con los criptoactivos sí tributarán. España, a falta de legislación específica, aplica las reglas generales de ganancias y pérdidas patrimoniales. Según reiteradas resoluciones a consultas vinculantes de la Dirección General de Tributos, la venta de criptomoneda a cambio de euros genera una ganancia o pérdida patrimonial por la diferencia entre el valor de transmisión y el valor de adquisición. Incluso la permuta de una criptomoneda por otra distinta constituye un hecho imponible: se considera que se enajena un elemento patrimonial –la primera criptomoneda– por el valor de mercado de lo que se recibe –la segunda criptomoneda–, surgiendo ganancia o pérdida que debe integrarse en la base del ahorro. Esto implica que, aunque alguien nunca vuelva a convertir sus bitcoines a euros, si los intercambia por otros tokens o los utiliza para comprar bienes, está realizando hechos imponibles sujetos a IRPF.

En la gestión de estas ganancias, Hacienda exige una trazabilidad completa del historial de transacciones para calcular la ganancia con método FIFO –*primero en entrar, primero en salir*–. El contribuyente debe poder acreditar los precios y fechas de adquisición de sus criptomonedas, lo cual se vuelve complejo si ha operado de forma anónima o en múltiples plataformas. De hecho, la Agencia Tributaria ha advertido sobre la dificultad de obtener esa información cuando las criptoactivos están en *wallets* personales o dispersas en *exchanges* extranjeros. No obstante, la carga de la prueba recae en el contribuyente: si declara pérdidas, por ejemplo, debe justificarlas con documentación fiable. Un usuario que compró bitcoin con un cupón anónimo y luego lo vendió con pérdida podría encontrarse en apuros para demostrar el costo de adquisición si no conserva el justificante del cupón y la

(42) Diferente sería si lo que se vendiese fuese un bien o servicio pagadero en bitcoin –ahí hay IVA–, pero la mera conversión de dinero a cripto no tributa por IVA. Desde una perspectiva más detallada, Ehrke Rabel y Zechner han explorado las dificultades normativas que implica gravar los servicios de intermediación de criptomonedas, en especial cuando la retribución del *exchange* se percibe en criptoactivos o se estructura mediante comisiones en tokens, lo que complica su delimitación como servicios financieros exentos o no sujetos a IVA. EHRKE RABEL, T.; ZECHNER, L., «VAT Treatment of Cryptocurrency Intermediation Services», *Intertax*, vol. 48, n.º 5, 2020.

información de canje. Este es un riesgo fiscal de operar en la opacidad: puede dificultar la justificación ante una inspección, incluso aunque no haya mala fe.

Conviene mencionar que las criptomonedas no son consideradas valores negociables cotizados, por lo que ciertas normas fiscales específicas para acciones no aplican. Por ejemplo, la regla anti-aplicación de pérdidas por recompra en dos meses –para valores homogéneos– no se estima aplicable a criptoactivos según la Dirección General de Tributos, al no calificarlas como valores. En cambio, podría aplicarse la regla general anti-aplicación de pérdidas por recompra en el plazo de un año –artículo 33.5 e) LIRPF)– si se considera que son «elementos patrimoniales homogéneos» –una cuestión discutida doctrinalmente–. En cualquier caso, las ganancias en criptoactivos tributan en la base del ahorro a tipos entre 19 por ciento y 26 por ciento, y las pérdidas pueden compensarse con otras ganancias patrimoniales bajo las reglas usuales.

En el Impuesto sobre el Patrimonio las criptomonedas están sujetas al Impuesto sobre el Patrimonio (IP) como cualquier otro bien. La Dirección General de Tributos ha aclarado que se deben valorar por su precio de mercado a 31 de diciembre de cada año (43). Muchos contribuyentes españoles han de incluir, en la declaración de patrimonio, el saldo de criptodivisas que posean al cierre del año, siempre que su base imponible total supere los mínimos exentos –recordando que en algunas CCAA este impuesto está bonificado, como Madrid, pero otras no–. La cuestión problemática es la comprobación: dado el anonimato, Hacienda puede desconocer la existencia del activo si no es declarado. Sin embargo, como veremos, desde 2023 se han establecido modelos informativos que obligan a terceros y a los propios contribuyentes a informar de estas tenencias, reduciendo la opacidad.

---

(43) En las resoluciones a consultas V0250-18 y V0590-18 el centro directivo confirma la sujeción al IP de la tenencia de criptomonedas en los siguientes términos: «Consiguientemente, los «bitcoines» y demás criptomonedas deberán declararse en el Impuesto sobre el Patrimonio por su precio de mercado determinado a fecha de devengo (31 de diciembre de cada año), de acuerdo, respectivamente, con lo artículos 24 y 29 de la Ley». La titularidad de un *wallet* de criptomonedas es también observada por la Dirección General de Tributos, en su consulta V2289-18, dispone lo siguiente: «Desde la perspectiva del Impuesto sobre el Patrimonio, habrán de declararse junto con el resto de los bienes de titularidad de la persona física, de la misma forma que se haría con un capital en divisas, valorándose en el impuesto a precio de mercado a la fecha del devengo, es decir, a 31 de diciembre de cada año (artículo 24 de la Ley 19/1991, de 6 de junio, que regula el impuesto), en definitiva, por su valor equivalente en euros a dicha fecha.

Obligaciones informativas –Modelos 172, 173, 721–: Una de las consecuencias de la Ley 11/2021 fue habilitar a la Administración para requerir información sobre criptoactivos. Se añadieron disposiciones en la Ley General Tributaria para forzar a *exchanges* y custodios a informar de saldos y operaciones de clientes, y a contribuyentes a declarar posesión de cripto en el extranjero. Tras desarrollos reglamentarios, en 2023 el Ministerio de Hacienda aprobó los modelos oficiales: el Modelo 172 –declaración anual de saldos en monedas virtuales–, el Modelo 173 –declaración anual de operaciones con criptomonedas– y el Modelo 721 –declaración de monedas virtuales situadas en el extranjero, análogo al antiguo Modelo 720– (44).

El Modelo 172 debe ser presentado por empresas –residentes en España– que custodien criptomonedas de terceros o que faciliten la tenencia –por ejemplo, *exchanges* con cuentas de cliente–, informando del saldo de criptoactivos de cada cliente a 31 de diciembre y el saldo medio del último trimestre. El Modelo 173, también a cargo de empresas, informa de las operaciones realizadas por sus clientes: adquisiciones, transmisiones, permutas, entre otros, con detalle de importes, fechas y contravalores. Por último, el Modelo 721 impone a personas físicas residentes declarar las criptomonedas que mantengan en *exchanges* o *wallets* extranjeros si superan ciertos umbrales –en 2023, todo indicaba que cualquier saldo menor a cincuenta mil euros debía informarse, similar a lo que era el 720 para cuentas, aunque tras la sentencia del TJUE que sancionó el régimen sancionador del 720, las multas se han moderado–. Cabe destacar que, a diferencia del 720 original, las criptomonedas en *cold wallets* propias no situadas en extranjero no encajarían en la definición –pues no hay «entidad gestora» extranjera–, pero si se custodian en un *exchange* fuera de España sí.

Estas obligaciones informativas significan que la Hacienda española obtendrá datos masivos sobre los titulares de criptomonedas. Un usuario que creyera mantener el anonimato comprando bitcoin con cupones puede verse descubierto a posteriori si, por ejemplo, transfiere esos bitcoines a un *exchange* que luego informa de su identidad y movimientos vía Modelo 173. Incluso si no lo hace, el

(44) El Modelo 721 es una declaración informativa obligatoria para residentes fiscales en España que posean criptomonedas en plataformas o wallets extranjeros, siempre que el valor total de estos activos supere los 50.000 euros a 31 de diciembre; su objetivo es controlar la tenencia de criptoactivos fuera del país y prevenir el fraude fiscal, debiendo incluirse datos identificativos del titular, del proveedor extranjero y de cada tipo de criptomoneda, y su incumplimiento puede conllevar sanciones económicas elevadas. [Consultado el 15 de octubre de 2025]. Disponible en: https://sede.agenciatributaria.gob.es/Sede/procedimientoini/GI55.shtml#:~: text=, virtuales%20%C2%B7%20Modelo%20179.

propio deber del Modelo 721 lo obliga a autoinculparse, por así decir, bajo riesgo de sanción –que tras la jurisprudencia europea ya no es confiscatoria, pero sigue existiendo–.

Si las ganancias con bitcoin alcanzan grandes cuantías y hay ocultación deliberada, podría configurarse un delito fiscal –artículo 305 CP– si se defraudan más de ciento veinte mil euros de cuota (45). También, si bitcoin se emplea como medio de pago en adquisiciones de bienes, la administración podría gravar la operación subyacente –por ejemplo, ITP si se compra un bien mueble de segunda mano con bitcoin, aunque esto es terreno poco explorado–.

Resumiendo, fiscalmente la compra de bitcoin con un *voucher* no genera por sí tributo inmediato, pero marca el inicio de una inversión cuyas rentas futuras deberán declararse –IRPF por ganancias– y cuyo valor puede estar sujeto a patrimonio. La utilización de medios anónimos no exime de la tributación y la falta de rastro bancario no impide que surjan obligaciones: de hecho, Hacienda está creando nuevos mecanismos para rastrear las criptomonedas independientemente de cómo se adquirieron. La opacidad inicial puede dar una falsa sensación de evasión, pero si en algún punto los criptoactivos salen a la luz –por ejemplo, para comprar un inmueble o convertir a euros–, se exigirá explicar su origen y tributar lo que corresponda. La colusión de lo fiscal y lo penal aparece cuando la ocultación es deliberada y cuantiosa, como se verá en el epígrafe de delitos tributarios.

---

(45) La idoneidad del fraude fiscal como delito previo al blanqueo de capitales ha generado intensos debates doctrinales y jurisprudenciales centrados en determinar si las conductas típicas del blanqueo -adquisición, tenencia, utilización, conversión o transmisión de activos- constituyen automáticamente un segundo delito o requieren elementos subjetivos adicionales. Esta controversia plantea serios problemas respecto a la prohibición del *non bis in idem* y ha propiciado reinterpretaciones del derecho penal incompatibles con los principios fundamentales de criminalidad. Adicionalmente, la delimitación de los bienes susceptibles de blanqueo presenta complejidades particulares, dado que se trata de activos originalmente en posesión del infractor y de naturaleza pecuniaria, circunstancia que podría determinar la exoneración del sospechoso por aplicación del principio de presunción de inocencia. NIETO MONTERO, J. J., «Monedas virtuales en la Directiva 2018/843, su tributación y blanqueo.», en *X Congreso Internacional sobre prevención y represión del blanqueo de dinero y IV Congreso de la Asociación Iberoamericana de Derecho penal económico y de la empresa: Ponencias y conclusiones del congreso. El blanqueo en la Unión Europea, su incidencia en el mundo digital y la internacionalización del Derecho penal, celebrado en la Facultad de Derecho de la Universidad de Santiago de Compostela, en julio de 2024, València*: Tirant lo Blanch, 2025, 2025, pp. 623-624.

VIII. TIPOLOGÍA DE EVENTUALES INFRACCIONES PENALES, TRIBUTARIAS Y ADMINISTRATIVAS

El empleo de medios de pago no rastreables para la adquisición de bitcoin puede dar lugar, dependiendo de la intencionalidad y circunstancias, a la comisión de distintos ilícitos penales y administrativo-tributarios. En este epígrafe se examinan las principales figuras delictivas e infracciones que podrían concurrir, distinguiendo entre delitos financieros, delitos fiscales y otras infracciones administrativas en materia tributaria o de control.

1. **Blanqueo de capitales en el ecosistema cripto: delito de blanqueo, prevención de blanqueo, *vouchers, Travel Rule, AML* y *MiCA***

A modo de marco general, este subepígrafe ofrece una visión integrada del delito de blanqueo aplicado a criptoactivos. Partimos del análisis del artículo 301 CP y de su evolución para, después, situar los vectores técnicos que condicionan la prueba y tienen incidencia en la determinación del elemento subjetivo. Prestamos especial atención al papel de los *vouchers* o cupones prepago como eslabón opaco de entrada y al efecto estudiamos la «Travel Rule» en la trazabilidad y la cooperación entre proveedores. El análisis se articula en conexión con el marco AML y con MiCA, destacando cómo ambos inciden en la tipicidad y la diligencia debida. Sobre ese diagnóstico, se identifican carencias –con especial relevancia de las existentes en la regulación de la prueba– y de coordinación administrativo-penal y se proponen medidas de *lege ferenda* para reforzar la seguridad jurídica sin sacrificar el desarrollo tecnológico.

1.1 El tipo penal de blanqueo de capitales y su aplicación a operaciones con criptomonedas

El artículo 301 del Código Penal español configura el delito de blanqueo de capitales mediante una tipificación que abarca la adquisición, posesión, utilización, conversión o transmisión de bienes procedentes de actividad delictiva. La conducta típica se perfecciona cuando el sujeto activo realiza estas acciones con conocimiento del origen ilícito de los bienes y con la finalidad de ocultar o encubrir su procedencia criminal, o de ayudar a la persona

que haya participado en la infracción a eludir las consecuencias legales de sus actos (46).

La reforma operada por la Ley Orgánica 6/2021 introdujo modificaciones sustanciales en la configuración del tipo. Particularmente relevante resulta que no se exige ya que el acto de ocultación sea exitoso; la mera finalidad y la consciencia del origen ilícito configuran el delito. Esta modificación amplía considerablemente el ámbito de punibilidad, abarcando tentativas de blanqueo que anteriormente podían quedar impunes. Así, cuando un sujeto utiliza *vouchers* prepagados para adquirir criptoactivos con conocimiento de que el efectivo proviene de actividades delictivas –paradigmáticamente, el tráfico de estupefacientes–, incurre en la conducta típica independientemente del éxito de la operación de lavado (47).

La reforma también introdujo agravantes específicas que elevan sustancialmente el marco punitivo –de tres años y tres meses hasta seis años de prisión– cuando el responsable ostenta la condición de sujeto obligado conforme a la normativa de prevención del blanqueo. Esta categoría incorpora expresamente, desde la entrada en vigor del Real Decreto-ley 7/2021, a los proveedores de servicios de cambio entre monedas virtuales y monedas de curso legal. La agravante se fundamenta en la especial posición de garante que ostentan los proveedores de servicios en el sistema de prevención del blanqueo, no hay más sujetos a los que agarrarse.

El ordenamiento penal español distingue diversas modalidades de blanqueo que resultan particularmente relevantes en el contexto de las operaciones con criptoactivos. Para empezar, debemos hablar de blanqueo propio y autoblanqueo. El artículo 301.1 CP tipifica el blanqueo realizado por terceros ajenos al delito precedente, mientras que el apartado 3 sanciona el autoblanqueo, esto es, cuando el propio autor del delito previo procede al lavado de los fondos obtenidos. Esta

---

(46) Como síntesis introductoria, se puede la revisión general sobre criptomonedas y BC/FT en España del profesor Hinojal. Hinojal, A., «Criptomonedas y blanqueo de capitales», *Logos Guardia Civil: Revista Científica del Centro Universitario de la Guardia Civil,* n.º 1, 2023, p.p. 215-240.

(47) Los vales y tarjetas prepago operan como eslabón opaco de entrada y salida que dificulta la trazabilidad y favorece operar con fondos ilícitos. En el interesantísimo articulo «Laundering the Profits of Ransomware» se analiza la operativa de los secuestradores de sistemas informáticos, que exigen un pago para desencriptar los programas de uso básico en las empresas. En dicha operativa se ha utilizado el sistema de cupones para ocultar los pagos de las víctimas. Usters, B.; Oerlemans, J.-J.; Pool, R., «Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies», *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 28, n.º 2, 2020, pp. 121-152.

modalidad, introducida en 2010 anticipándose a las exigencias de la normativa europea, resulta especialmente frecuente en la práctica de adquisición de bitcoin con medios no rastreables, donde previo delito inicial se convierte el resultado monetario de moneda de curso legal en activos digitales.

El párrafo último del artículo 301.1 CP sanciona las conductas de blanqueo realizadas por imprudencia grave. Esta modalidad típica adquiere especial relevancia en supuestos donde operadores de servicios de cambio aceptan reiteradamente cupones o *vouchers* omitiendo controles básicos de diligencia debida (48).

La conversión de dinero de origen ilícito en *vouchers* y, después, en criptomonedas cuadra perfectamente en la definición típica de blanqueo como forma de ocultación, encontrando respaldo normativo adicional en la Directiva (UE) 2018/1673, que enfatiza expresamente que el uso de monedas virtuales presenta nuevos riesgos de blanqueo que deben ser adecuadamente abordados (49).

El espectro de delitos susceptibles de generar productos para el blanqueo se ha ampliado considerablemente. El marco normativo actual incluye todo delito grave y, de manera expresa, los delitos fiscales. Sin ir más lejos, la Ley 10/2010 de prevención del blanqueo de capitales incorporó la cuota defraudada en los delitos contra la

---

(48) La delimitación entre dolo eventual e imprudencia constituye una cuestión probatoria compleja pero determinante, especialmente en casos donde no existe evidencia concluyente de intencionalidad directa. El dolo eventual implica que el sujeto prevé la posibilidad de que su conducta cause un resultado ilícito –por ejemplo, que los fondos provengan de actividades delictivas– y, aun así, decide actuar, aceptando ese riesgo. Estaríamos ente el caso de un *exchange* que sospecha que los cupones que recibe podrían tener origen ilícito, pero los acepta igualmente porque le interesa la ganancia. La imprudencia grave ocurre cuando el sujeto no prevé el resultado ilícito, pero debería haberlo hecho si hubiera actuado con la diligencia exigible. No hay aceptación del riesgo, sino descuido o negligencia grave. En este caso el *exchange* por desidia, omite verificar la procedencia de los cupones, sin tener indicios concretos de ilegalidad. No siempre hay pruebas directas de la intención del sujeto. Los tribunales deben determinar el estado mental del acusado a partir de la frecuencia y volumen de las operaciones, la naturaleza de los clientes, la existencia de alertas previas o señales de riesgo o del nivel de formación o experiencia del operador. La diferencia entre dolo eventual e imprudencia marca la frontera entre el delito doloso y el imprudente, lo que tiene consecuencias importantes en la pena.

(49) Esta norma europea, transpuesta al ordenamiento español, reconoce expresamente los riesgos asociados al uso de monedas virtuales en el contexto del blanqueo. En su considerando 6, señala que los Estados miembros deben abordar adecuadamente estos riesgos. Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32018L1673

Hacienda Pública como bienes procedentes de actividad delictiva. Esta ampliación tiene implicaciones prácticas significativas: la conversión de dinero evadido fiscalmente en bitcoines constituye igualmente delito de blanqueo (50).

La configuración típica del artículo 301 CP, caracterizada por su amplitud descriptiva, permite subsumir las conductas realizadas con cupones prepagados y criptoactivos sin requerir modificación legislativa. Los órganos jurisdiccionales han confirmado reiteradamente que los activos digitales constituyen «bienes» en el sentido técnico-jurídico del artículo 301 CP, equiparándolos funcionalmente a activos patrimoniales susceptibles de integrar operaciones de blanqueo.

La jurisprudencia del Tribunal Supremo ha establecido criterios hermenéuticos consolidados para la aplicación del tipo penal a las operaciones con criptomonedas. La Sentencia 326/2019 marcó un hito interpretativo al caracterizar Bitcoin como bien mueble de naturaleza inmaterial. El Alto Tribunal precisó que, aunque estos activos no constituyen moneda de curso legal, resultan plenamente aptos para integrar conductas típicas de blanqueo cuando se emplean instrumentalmente para dificultar la trazabilidad de fondos procedentes de delitos precedentes (51).

La evolución jurisprudencial alcanzó un punto de inflexión con la STS 224/2024, que delimitó con precisión los contornos típicos del delito. Esta resolución rechazó interpretaciones extensivas que criminalicen operaciones meramente neutrales, estableciendo que el

---

(50) Por ejemplo, cuando un sujeto defrauda 200.000 euros en concepto de IVA no declarado y posteriormente adquiere bitcoines con ese dinero para ocultar su origen, incurre en blanqueo de capitales con fondos procedentes de actividad fiscal delictiva. Esta extensión del tipo refleja la evolución hacia una concepción omnicomprensiva del blanqueo que abarca cualquier forma de legitimación de activos de origen criminal. En IVA, la sentencia Hedqvist delimita la exención aplicable y la doctrina reciente matiza su extensión a NFTs y servicios asociados, con implicaciones recaudatorias. NESS, S., «VAT/GST Harmonisation Challenges for Digital Assets such as Bitcoin and NFTs in the EU (following C-264/14 Hedqvist)», *Journal of Business Economics and Management*, 2024.

(51) En este caso, el Tribunal Supremo enfrentó un delito de estafa relacionado con bitcoines y, aunque el asunto principal era defraudatorio, el fallo dedicó consideraciones a la naturaleza del bitcoin. Afirmó que no es moneda de curso legal, sino «activo de contraprestación», fijando la calificación de las criptodivisas. Ahora bien, aunque en el caso no se trató el blanqueo, esta sentencia ha sido la referencia en casos posteriores para entender qué se está blanqueando cuando se blanquea «dinero» convertido a bitcoines: se blanquean bienes, activos patrimoniales, no moneda en sentido técnico, pero la conducta encaja igualmente en el delito de blanqueo porque el artículo 301 CP se refiere a bienes procedentes de delito.

tipo penal exige la concurrencia de dolo específico de ocultación. La sentencia clarificó que no constituye blanqueo la mera facilitación de la introducción en el mercado regular de fondos que requieren legitimación por su origen delictivo. Por el contrario, debe acreditarse una conducta posterior, autónoma y diferenciada, orientada específicamente a legitimar bienes previamente obtenidos de forma ilícita.

1.2 El tipo penal de blanqueo de capitales frente a las características técnicas de los criptoactivos

El marco penal vigente demuestra una notable capacidad de adaptación ante las características de los criptoactivos. La descentralización inherente a estos sistemas, que excluye el control bancario tradicional, encuentra respuesta adecuada en la configuración típica del artículo 301 CP. La norma no exige la participación de intermediarios específicos, abarcando cualquier modalidad de conversión o transmisión de bienes de origen ilícito, independientemente del canal empleado.

En principio, la irreversibilidad de las transacciones registradas en *blockchain*, aunque dificulta significativamente la recuperación de activos blanqueados, no constituye impedimento para la aplicación del tipo penal. El delito se consuma con la realización de la conducta típica, independientemente del éxito final en la ocultación del origen ilícito de los fondos. También el tipo hace que el pseudoanonimato característico de las transacciones *blockchain* en las monedas virtuales «clásicas», como bitcoin, no constituya un obstáculo jurídico ni técnico insuperable (52). La reforma de 2010 incorporó la mera tenencia o posesión consciente de bienes de origen criminal, permitiendo perseguir conductas que anteriormente escapaban al ámbito punitivo (53). El elemento subjetivo del tipo no requiere un conocimiento exhaustivo del delito precedente. Esto hace que las posibilidades de segmentación de las cuantías mediante técnicas

(52) El pseudoanonimato de bitcoin permite reconstruir los recorridos transaccionales, pero no garantiza anonimato absoluto; los primeros análisis de la red y la evidencia empírica sobre usos ilícitos lo demuestran. Foley, S.; Karlsen, J. R.; Putniņš, T. J., «Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?», *The Review of Financial Studies*, vol. 32, n.º 5, 2019, pp. 1798-1853, DOI: 10.1093/rfs/hhz015.

(53) Conforme estableció la STS 501/2019, resulta suficiente la certeza sobre la procedencia delictiva de los bienes, sin exigirse una descripción pormenorizada de la actividad delictiva anterior.

sofisticadas como el pitufeo o *smurfing* digital o la utilización de múltiples direcciones *wallet* también encuentren cobertura típica (54).

Ahora bien, la extensión y adaptabilidad del tipo del blanqueo de capitales no significa falta de límites. La jurisprudencia ha desarrollado una línea que limita la aplicación indiscriminada del tipo penal a las operaciones con criptomonedas. La STS 10/2024 estableció que el blanqueo de capitales no constituye un delito de sospecha, exigiendo prueba rigurosa de todos los elementos típicos, incluido el origen criminal de los bienes objeto de blanqueo (55). Esta doctrina adquiere especial relevancia en el contexto de los criptoactivos, donde la trazabilidad técnica garantizada por *blockchain* no se traduce automáticamente en trazabilidad jurídica eficaz para la determinación de responsabilidades penales. La inmutabilidad del registro distribuido proporciona la pura certeza sobre las transacciones realizadas, pero no sobre la identidad de los intervinientes, ni sobre el elemento volitivo del tipo.

La operativa indicada en la primera parte del artículo no permite determinar fácilmente la concurrencia del elemento subjetivo del tipo. Esta limitación probatoria constituye uno de los principales desafíos para la persecución eficaz del blanqueo mediante criptoactivos.

1.3 Carencias del artículo 301 CP

Así, la principal deficiencia del artículo 301 CP en su aplicación a operaciones con vouchers de criptomonedas y criptomonedas radica en las dificultades probatorias específicas que plantea la operativa. La adquisición de manera anónima de vouchers o cupones en pequeñas cantidades segmentando los fondos es el primer paso en difuminar al elemento subjetivo (56). Y cuando se produce el paso

(54) En la sentencia 335/2010 del Tribunal Supremo, Sala Segunda, de 19 de junio de 2010 se analiza la aplicación del artículo 301 del Código Penal, destacando que la mera posesión de bienes ilícitos con conocimiento de su origen delictivo es suficiente para configurar el delito de blanqueo, incluso sin operaciones de transformación o encubrimiento.

(55) La STS 10/2024, dictada por la Sala Segunda del Tribunal Supremo el 11 de enero de 2024, establece que el delito de blanqueo de capitales no puede fundarse en meras sospechas, exigiendo una prueba rigurosa de todos los elementos típicos, especialmente del origen criminal de los bienes objeto de blanqueo. La sentencia subraya que el artículo 301 del Código Penal no puede aplicarse de forma automática sin acreditar la existencia de una actividad delictiva concreta y el conocimiento del acusado sobre dicha procedencia ilícita, reforzando así las garantías procesales y limitando la extensión del tipo penal en casos con indicios débiles o sin conexión probada con un delito precedente.

(56) La adquisición anónima de criptoactivos mediante *vouchers* prepagados inferiores a 150 euros –umbral establecido por la Quinta Directiva AML– evidencia

del voucher a la criptomoneda, aunque las transacciones quedan registradas públicamente de forma inmutable, el pseudoanonimato de las direcciones *wallet* imposibilita la identificación directa de los titulares, generando lagunas probatorias significativas respecto al elemento subjetivo del tipo. Además, se le pueden añadir más capas de ocultación como la utilización de *mixers*, *tumblers* o protocolos CoinJoin, que diluyen la trazabilidad sin vulnerar directamente el tipo penal. Estas tecnologías dificultan extremadamente la acreditación del nexo causal entre los fondos de origen ilícito y las transacciones posteriores. Y añadir más fragmentación, no solo la de la adquisición de cupones, sino una fragmentación de operaciones ya con el criptoactivo, mediante múltiples transacciones de importe reducido para explotar las limitaciones del principio de insignificancia penal (57). La descoordinación entre el marco preventivo y el penal en cuestiones de blanqueo de capitales reduce sustancialmente la eficacia del artículo 301 CP en este ámbito: si bien la Ley 10/2010 impone a los proveedores de servicios sobre criptoactivos obligaciones de diligencia debida y comunicación de operaciones sospechosas al SEPBLAC, persisten lagunas estructurales significativas (58).

Los nuevos modelos informativos tributarios 172, 173 y 721, de los que ya hemos hablado, permiten rastrear operaciones con criptoactivos, pero su eficacia se circunscribe a exchanges regulados y plataformas cooperativas. Las transacciones *peer-to-peer* y los intercambios en mercados descentralizados (DEX) que operan mediante *smart contracts* autónomos quedan fuera del perímetro de

---

otra brecha significativa. La prevención administrativa fracasa en estos supuestos al no capturar el rastro inicial de conversión de efectivo a criptoactivos.

(57) En la STS 224/2024, de 7 de marzo (ponente Excmo. Sr. D. Julián Sánchez Melgar), se absuelve al acusado por blanqueo de capitales imprudente (art. 301.3 CP) al considerar atípica la conducta de permitir el uso de su cuenta para recibir 850 euros procedentes de una estafa. El Tribunal aplica el principio de insignificancia y exige una imprudencia cualificada, destacando que la escasa cuantía y la pasividad del sujeto excluyen la tipicidad penal.

(58) Como veremos más adelante, si bien la Travel Rule del Reglamento (UE) 2023/1113 es un avance importante, presenta limitaciones técnicas relevantes. La normativa obliga a transmitir información del ordenante y beneficiario en transferencias de criptoactivos, pero incluye una excepción para las wallets frías donde el usuario mantiene el control directo de sus claves privadas. Precisamente estos instrumentos constituyen el vector preferente para preservar el anonimato en operaciones ilícitas. El artículo 16 del Reglamento introduce medidas reforzadas cuando las transferencias implican wallets frias. El proveedor debe verificar la identidad del titular de la wallet si la transferencia supera los 1.000 euros en estos casos.

control. Esta limitación genera un efecto desplazamiento hacia plataformas no reguladas sin impedir materialmente las conductas de blanqueo.

1.4 Propuestas de *lege ferenda*

Se podría proponer una agravante específica en el artículo 301 CP para sancionar con mayor severidad el blanqueo realizado mediante el uso de la técnica mixta de ocultación a la que nos hemos referido: una primera parte utilizando cupones o *vouchers* que se compran con efectivo y sin dejar rastro y una segunda en la que se utilizan tecnologías de mejora del anonimato me parece objetable, alineada con la definición establecida en el Reglamento (UE) 2024/1624, aplicable a partir del 10 de julio de 2027 (59). La agravante abarcaría el uso doloso de los cupones y de servicios de mezcla (*mixers* y *tumblers*), *atomic swaps*, *zero-knowledge proofs* y criptomonedas orientadas a la privacidad (*Monero*, *Zcash*) cuando se utilicen específicamente para blanquear fondos de origen delictivo (60).

La propuesta respetaría el principio de neutralidad tecnológica, porque no criminaliza el uso de tecnologías anonimizadora, sino que agrava exclusivamente su utilización dolosa en contexto de blanqueo. Esta aproximación resulta coherente con el enfoque del Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, que no prohíben estas tecnologías, pero establece controles para su utilización (61).

Sin embargo, la introducción de esta agravante tiene significativas objeciones. En primer lugar, existe un riesgo de vulneración del

(59) Que caracteriza las «monedas de mejora del anonimato» como aquellos criptoactivos con características integradas concebidas para hacer anónima la información sobre transferencias, ya sea de forma sistemática u optativa. Este Reglamento europeo refuerza significativamente la posición jurisprudencial española al establecer un régimen considerablemente más estricto para los criptoactivos que implementan funcionalidades de privacidad avanzada. La normativa introduce definiciones precisas que proporcionan base jurídica sólida para la diferenciación normativa de estos instrumentos cuando se emplean con fines ilícitos.

(60) Esta medida estaría en armonía en las recomendaciones del GAFI, que cataloga el uso de servicios de anonimización como indicador de alto riesgo de blanqueo. La reforma permitiría elevar las penas hasta el límite superior previsto para conductas agravadas (prisión de tres años y tres meses a seis años) cuando se demuestre intencionalidad específica de ocultación.

(61) En concreto, en sus «considerandos» 22 y 23, lo fundamenta, y en varios artículos se establecen esas medidas de control (artículos 3, 14 y 16).

principio *non bis in idem*, dado que la esencia del artículo 301 CP radica precisamente en la ocultación o encubrimiento del origen ilícito. Esta eventual duplicidad ha sido reseñada ya por la doctrina respecto a propósito de otros mecanismos de ocultación en el blanqueo de capitales (62). Establecer una agravante por utilizar este tipo de operativas que incrementan esa capacidad de ocultación podría constituir un bis *in idem* material, al sancionar doblemente la misma cualidad intrínseca de la conducta típica (63).

También sería un punto a estudiar la reforma de la aplicación del principio de insignificancia en delitos de blanqueo por la técnica mixta de la utilización de cupones y, a través de ellos, adquirir criptoactivos, mediante la introducción de criterios específicos que consideren la naturaleza acumulativa de las operaciones. La propuesta establecería que, cuando se detecte fraccionamiento deliberado de operaciones en importes individualmente insignificantes, se compute el valor total acumulado para determinar la relevancia penal. Esta reforma haría necesario incluir un apartado específico que establezca que el principio de insignificancia no operará cuando el fraccionamiento de operaciones con criptoactivos obedezca al propósito de eludir umbrales penales, siempre que se acredite unidad de propósito, proximidad temporal y homogeneidad de medios (64).

Otra sugerencia de *lege ferenda* sería incluir en la responsabilidad penal de las personas jurídicas un régimen de responsabilidad penal para entidades que emitan *vouchers* sobre criptoactivos o presten servicios de «anonimización» sobre criptoactivos e incumplan deliberadamente las obligaciones de prevención del blanqueo. La reforma ampliaría las accesorias del artículo 302 del Código Penal para incluir la suspensión temporal de licencias para operar con criptoactivos, la prohibición de emitir

(62) Muñoz Marín, A., «Blanqueo de capitales en los supuestos de tráfico de drogas por el mismo sujeto: el autoblanqueo y el principio non bis in ídem», *CEFLegal: Revista práctica de derecho. Comentarios y casos prácticos*, n.º 162, 2014, pp. 212-216.

(63) Como alternativas, cabría reconocer que la utilización de estas operativas se traduce únicamente en la graduación de la pena dentro del tipo básico o como elemento en la categoría de la culpa, sin configurar una agravante específica autónoma.

(64) Ya hemos comentado anteriormente que el elemento subjetivo del tipo del 301CP, no requiere un conocimiento exhaustivo del delito precedente, esto hace que se pueda combatir la segmentación de las cuantías mediante técnicas sofisticadas como el pitufeo o *smurfing* digital o no -como pasa con los vouchers- y la utilización de múltiples direcciones wallet. Sin embargo, dejar claro el tratamiento de la segmentación, como ocurre en la normativa de limitación de pagos en efectivo creo que es prudente y evita dejar un margen que puede tornarse difuso.

cupones, así como la inhabilitación para gestionar fondos digitales por períodos comprendidos entre dos y diez años (65).

1.5 La Quinta Directiva 2018/843 antiblanqueo, el Reglamento MiCA y su impacto en el artículo 301 del Código Penal

La Directiva (UE) 2018/843, conocida como Quinta Directiva antiblanqueo, representa un punto de inflexión fundamental en la integración de los criptoactivos dentro del marco europeo de prevención del blanqueo de capitales y financiación del terrorismo. Esta normativa, que entró en vigor el 10 de enero de 2020, estableció por primera vez la incorporación expresa de los proveedores de servicios de criptomonedas como sujetos obligados en la legislación europea, creando un precedente regulatorio de alcance transformador para la armonización de controles antiblanqueo en el ámbito digital (66).

La directiva, para empezar, introduce definiciones técnico-jurídicas precisas que resultan esenciales para delimitar el objeto material del delito de blanqueo cuando se emplean criptoactivos. El concepto de «monedas virtuales» se define como representaciones digitales de valor no emitidas ni garantizadas por un banco central ni por una autoridad pública, no necesariamente asociadas a una moneda establecida legalmente, que carecen del estatuto jurídico de moneda o dinero, pero que son aceptadas por personas físicas o jurídicas como medio de cambio y pueden transferirse, almacenarse y negociarse por medios electrónicos. Esta caracterización normativa proporciona seguridad jurídica indispensable para la correcta aplicación del artículo 301 CP, eliminando las incertidumbres interpretativas que anteriormente debilitaban la persecución penal efectiva (67).

---

(65) Estas propuestas se coordinarían con el marco administrativo. De este modo, se configuraría un sistema integral de responsabilidad que combina sanciones penales con medidas administrativas preventivas, fortaleciendo la capacidad del ordenamiento jurídico para combatir eficazmente el blanqueo de capitales a través de criptoactivos.

(66) España transpuso la Quinta Directiva mediante el Real Decreto-ley 7/2021, introduciendo modificaciones sustanciales en la Ley 10/2010 de prevención del blanqueo de capitales. La transposición española adoptó una aproximación maximalista que superó los estándares mínimos exigidos por la normativa europea. El legislador nacional no solo incluyó a los proveedores de cambio cripto-monedas de curso legal y wallets, sino que extendió las obligaciones al intercambio entre diferentes monedas virtuales, anticipándose así a desarrollos normativos posteriores y estableciendo un marco regulatorio más comprehensivo.

(67) Esta definición delimita el objeto material del delito de blanqueo cuando se emplean criptoactivos, permitiendo identificar con claridad qué tipo de bienes

La normativa incorpora los conceptos de proveedores de servicios de criptomonedas como sujetos obligados comprende dos categorías específicas: los proveedores de servicios de cambio entre monedas virtuales y moneda curso legal (68) y los proveedores de servicios de wallets o monederos de custodia. Esta inclusión trasciende el ámbito meramente administrativo para configurarse como elemento de base de la normativa administrativa, pero su repercusión es limitada (69).

Como deriva de esta normativa, se creó el Registro de Proveedores de Servicios de Criptoactivos en el Banco de España, pero desde el 30 de diciembre de 2024 entró en vigor el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (Reglamento MiCA) y esta parte de la normativa quedó, por duplicación de obligaciones, derogada (70). MiCA establece un marco regulador integral y armonizado para los proveedores de servicios de criptoactivos en el ámbito de la Unión Europea, unificando los criterios de autorización y funcionamiento que hasta la fecha se encontraban dispersos en las diferentes legislaciones nacionales. Ahora, aquellos operadores que ofrecen servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos –anteriormente sujetos a la obligación de inscripción en el registro administrado por el Banco de España conforme a la disposición adicional segunda de la Ley 10/2010, de 28 de abril– quedan ahora sometidos al nuevo régimen europeo. En consecuencia, estos operadores deberán obtener la correspondiente autorización de la Comisión Nacional del Mercado de Valores (CNMV), designada como autoridad competente en España según lo dispuesto en el artículo 251 de la Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión.

---

digitales pueden ser objeto de ocultación, conversión o posesión consciente. También elimina la ambigüedad interpretativa que existía en torno a si los criptoactivos podían considerarse «bienes» a efectos del artículo 301 CP y refuerza la seguridad jurídica en la persecución penal, al permitir una subsunción clara en el tipo penal sin necesidad de analogías extensivas o interpretaciones forzadas.

(68) Fiat o fiduciaria, como la quieran denominar.

(69) Se daba publicidad al cumplimiento de los requisitos mínimos establecidos en la normativa de prevención del blanqueo de capitales. El régimen MiCA redefine obligaciones de los wallets de criptoactivos, con debate doctrinal sobre su idoneidad y riesgos regulatorios.

(70) Desde el 30/12/2024 el Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos, previsto en la disposición adicional segunda de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales, ha sido dejado sin efecto, pero subsiste a efectos informativos sobre aquellas inscripciones anteriores de esa fecha y que se encuentran en el régimen transitorio previsto en el artículo 143 del Reglamento MiCA.

Paralelamente, el 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, también aplicable desde el 30 de diciembre de 2024, elimina los requisitos de registro contemplados en la Directiva (UE) 2015/849 sobre prevención del blanqueo de capitales y financiación del terrorismo. Esta modificación normativa tiene como objetivo evitar la duplicación de obligaciones regulatorias y garantizar la coherencia del nuevo marco jurídico europeo. Así, el Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos ha quedado formalmente suprimido. No obstante, se mantiene con carácter meramente informativo respecto de aquellas inscripciones efectuadas con anterioridad al 30 de diciembre de 2024, las cuales pueden beneficiarse del régimen transitorio establecido en el artículo 143 del Reglamento MiCA (71).

Resulta pertinente señalar que el régimen jurídico de la Quinta Directiva presentaba un alcance significativamente limitado (72). Si bien la Ley 10/2010 configuraba a estos proveedores como sujetos obligados en materia de prevención del blanqueo de capitales, no contemplaba disposiciones relativas a la supervisión financiera prudencial, el gobierno corporativo, la seguridad tecnológica, la conducta de mercado o la transparencia informativa.

En este sentido, debe subrayarse que el Banco de España carecía de competencias para supervisar los riesgos financieros, operativos o tecnológicos asociados a estas actividades, así como de facultades en materia de conducta de mercado. Por consiguiente, la inscripción registral no constituía, en modo alguno, una aprobación o validación de las actividades desarrolladas por estos operadores, limitándose a certificar el cumplimiento de los requisitos mínimos establecidos en la normativa de prevención del blanqueo de capitales.

---

(71) El artículo 143 del Reglamento (UE) 2023/1114 (MiCA), relativo a los mercados de criptoactivos, que establece un régimen transitorio para los proveedores de servicios y emisores que ya operaban antes de su entrada en vigor. Dicho régimen permite continuar la actividad hasta el 1 de julio de 2026, siempre que se notifique a la autoridad competente y se solicite la autorización antes del 30 de julio de 2025. Los Estados miembros pueden acortar este plazo, como ha anunciado España, que prevé exigir el cumplimiento pleno del MiCA a partir de diciembre de 2025.

(72) La inscripción registral se encontraba condicionada exclusivamente al cumplimiento de dos requisitos: la implementación de procedimientos y órganos adecuados de prevención del blanqueo de capitales y financiación del terrorismo y la acreditación de honorabilidad comercial y profesional.

Volviendo a la Quinta Directiva, esta establece un sistema comprehensivo de obligaciones de identificación y verificación de clientes (Know Your Customer-KYC) que trasciende el ámbito administrativo para configurarse como presupuesto fundamental de la aplicación del derecho penal. Los proveedores de servicios de criptoactivos quedan sometidos a medidas de diligencia debida equivalentes a las exigidas a las entidades financieras tradicionales. Estas medidas comprenden la identificación formal del cliente y verificación fehaciente de su identidad, la identificación del titular real cuando el cliente actúe por cuenta de terceros, la obtención de información detallada sobre el propósito y naturaleza prevista de la relación comercial, y el seguimiento continuo y documentado de las operaciones realizadas.

El cumplimiento de estas obligaciones KYC incide directamente en la acreditación del elemento subjetivo del delito de blanqueo. Un proveedor que implementa adecuadamente los procedimientos de diligencia debida dispondrá de documentación que puede resultar exculpatoria en caso de investigación penal, demostrando la ausencia de conocimiento sobre el origen ilícito de los fondos. Por el contrario, el incumplimiento deliberado de estas obligaciones puede constituir indicio cualificado de participación dolosa en operaciones de blanqueo. La jurisprudencia española ha comenzado a consolidar una línea interpretativa que valora el grado de cumplimiento de las obligaciones preventivas como elemento determinante para establecer la concurrencia de dolo eventual en delitos de blanqueo mediante criptoactivos.

La normativa faculta expresamente a los Estados miembros para prohibir la circulación de tarjetas prepago anónimas emitidas en terceros países y reduce el umbral de anonimato de estas tarjetas de 250 a 150 euros. Esta reducción del umbral cierra vías tradicionales de adquisición anónima de criptoactivos que anteriormente facilitaban operaciones de blanqueo de menor cuantía, pero alta frecuencia, técnica conocida como *smurfing* digital (73).

En definitiva, el cumplimiento por parte de un proveedor de servicios de criptoactivos de los requisitos de inscripción establecidos en la Quinta Directiva (UE) 2018/843, transpuesta al ordenamiento

(73) La directiva establece umbrales específicos que modulan la intensidad de las medidas de diligencia debida aplicables. Las medidas simplificadas quedan expresamente excluidas para operaciones con criptoactivos, que la normativa cataloga como productos de riesgo inherentemente elevado. Esta categorización normativa tiene implicaciones penales relevantes, pues elimina la posibilidad de alegar desconocimiento basado en la aplicación de controles reducidos.

español mediante el Real Decreto-ley 7/2021, podría tener efectos relevantes en el ámbito penal, particularmente en casos de imputación por blanqueo de capitales. Aunque dicho cumplimiento no excluye automáticamente la responsabilidad penal, sí puede operar como elemento atenuante o incluso exculpatorio, dependiendo de las circunstancias del caso. La inscripción en el registro de la CMNV –anteriormente, en el BDE– y la aplicación efectiva de medidas de diligencia debida, identificación de clientes y reporte de operaciones sospechosas constituyen indicios de actuación conforme a la legalidad, lo que puede debilitar la presunción de dolo o conocimiento del origen ilícito de los fondos. En este sentido, el proveedor que haya cumplido con las exigencias normativas podría beneficiarse de una interpretación más favorable del tipo penal del artículo 301 del Código Penal, especialmente si demuestra colaboración con las autoridades o ausencia de voluntad de ocultación (74).

1.6 La *Travel Rule* y sus efectos en la aplicación del artículo 301 CP

La travel rule (o regla de viaje) es una norma de *soft law* del Grupo de Acción Financiera Internacional (GAFI/FATF) que busca prevenir el lavado de dinero y la financiación del terrorismo en el ámbito de los criptoactivos. Aunque originalmente fue diseñada para transferencias bancarias tradicionales, desde 2019 se ha extendido a los proveedores de servicios de activos virtuales (VASPs), como *exchanges* y wallets on line. Fue recogida por el Reglamento (UE) 2023/1113 relativo a la

(74) La jurisprudencia reciente, como la STS 10/2024, refuerza esta tesis al exigir prueba rigurosa del elemento subjetivo del delito, lo que permite valorar el cumplimiento normativo como factor que excluye la culpabilidad o atenúa la responsabilidad penal. La STS 10/2024, dictada por la Sala Segunda del Tribunal Supremo el 11 de enero de 2024 (Rec. 7241/2021), como hemos estado insistiendo, esta línea jurisprudencial limita el delito de blanqueo de capitales en lo que respecta al elemento subjetivo. El ponente, Excmo. Sr. D. Manuel Marchena Gómez, subraya que este delito no puede configurarse como un tipo de sospecha, sino que exige una prueba rigurosa y directa del dolo, es decir, del conocimiento efectivo del origen criminal de los bienes y de la voluntad de ocultarlos o integrarlos en el circuito económico legal tiene especial relevancia en el ámbito de los criptoactivos, donde la trazabilidad es limitada y el riesgo de automatismos acusatorios es alto. La STS 10/2024 exige que la imputación penal se funde en hechos probados y no en presunciones derivadas del uso de tecnologías descentralizadas o de anonimato. https://vlex.es/vid/977115458

información que acompaña a las transferencias de fondos y criptoactivos y ha devenido obligatoria desde el 30 de diciembre de 2024 (75).

El artículo 16 del Reglamento (UE) 2023/1113 introduce medidas reforzadas cuando las transferencias implican carteras autocustodiadas (self-hosted wallets). En estos casos, el proveedor debe verificar la identidad del titular de la wallet si la transferencia supera los 1.000 euros. Pero este umbral solo aplica a esa situación específica, no como regla general (76). Esta información debe incluir el nombre completo del ordenante y beneficiario, el número de cuenta o dirección de wallet correspondiente, la dirección física o identificador nacional único, y el nombre del CASP del beneficiario. La información debe «viajar» con la transacción y conservarse tanto en origen como en destino durante un período mínimo de cinco años, creando una cadena de trazabilidad documental que facilita significativamente la investigación judicial de delitos de blanqueo. A diferencia de la Quinta Directiva AML (UE) 2018/843, que sí contemplaba umbrales de anonimato (150 € para tarjetas prepago físicas y 50 € para remotas), el Reglamento 2023/1113 elimina tales umbrales para las transferencias de criptoactivos entre CASP.

El impacto de la travel rule en la aplicación efectiva del artículo 301 CP resulta significativo. La normativa permite superar las dificultades

---

(75) El núcleo normativo de esta obligación se encuentra en los artículos 14 a 17 del Reglamento. El artículo 14 establece las obligaciones de información aplicables a todas las transferencias de criptoactivos, incluyendo datos como el nombre, número de cuenta, dirección y documento identificativo tanto del originador como del beneficiario. El artículo 15 contempla excepciones limitadas, por ejemplo, en transferencias entre proveedores regulados dentro de la Unión Europea, siempre que se garantice la trazabilidad. El artículo 16 introduce medidas reforzadas de diligencia debida para las operaciones que involucren *wallets* no custodiadas, obligando al proveedor a verificar la identidad del titular de la *wallet*. Finalmente, el artículo 17 regula la conservación de los datos recopilados, que deben mantenerse durante cinco años y estar disponibles para las autoridades competentes.

(76) Existe una obligación general de trazabilidad. El reglamento impone a los proveedores de servicios de criptoactivos (CASP) la obligación de acompañar todas las transferencias de criptoactivos con información sobre el ordenante y el beneficiario, sin establecer un umbral general de exclusión como ocurría en normativas anteriores. No obstante, el límite de 150 euros sigue vigente en ciertos instrumentos de entrada al ecosistema cripto, como los cupones o tarjetas prepago, pero no aplica a las transferencias entre CASP bajo el Reglamento (UE) 2023/1113, pero, los proveedores de servicios de criptoactivos (CASP) están obligados a implementar sistemas de monitoreo y análisis de patrones transaccionales, que les permitan identificar operaciones sospechosas por su frecuencia, estructura o destinatarios comunes. En este sentido, el *pitufeo* o *smurfing* no solo debe ser detectado como técnica de ocultación, sino también informado como indicio de blanqueo, conforme a las obligaciones de comunicación de operaciones sospechosas previstas en la Ley 10/2010 y en el propio Reglamento.

probatorias tradicionales asociadas al blanqueo mediante criptoactivos, proporcionando a las autoridades investigadoras información identificativa precisa y verificable sobre los participantes en transacciones sospechosas. La obligación de conservar registros históricos completos permite reconstruir cadenas transaccionales complejas, facilitando la prueba del elemento objetivo del tipo penal –conversión o transmisión de bienes de origen ilícito– y proporcionando indicios robustos sobre el elemento subjetivo.

2. **Delitos contra la Hacienda Pública**

La adquisición de criptomonedas mediante cupones o efectivo constituye, desde una perspectiva jurídico-penal, una operación en principio neutra que no implica, por sí misma, la comisión de infracción alguna. Sin embargo, esta neutralidad se ve alterada cuando dicha operación se convierte en un medio comisivo integrado en una conducta delictiva de mayor entidad (77).

En primer lugar, la compra de bitcoin puede formar parte del *iter criminis* cuando se orienta deliberadamente a la defraudación tributaria conforme al artículo 305.1 del Código Penal. Esta modalidad delictiva comprende la elusión del pago de tributos, la obtención indebida de devoluciones o el disfrute fraudulento de beneficios fiscales, siempre que se supere el umbral de ciento veinte mil euros por cada tributo y período impositivo (78). Por tanto, en la práctica, la mera compra de

(77) En el ámbito de las obligaciones tributarias, la omisión deliberada de declarar plusvalías derivadas de operaciones de *trading*, *staking* o *swap* con bitcoin de procedencia anónima constituye delito fiscal cuando la cuota del Impuesto sobre la Renta de las Personas Físicas supera los ciento veinte mil euros en el ejercicio correspondiente, siendo de aplicación el artículo 305.1 del Código Penal. Asimismo, cuando se canalizan ventas sin factura hacia monederos no custodiados con el propósito de eludir la repercusión o ingreso del Impuesto sobre el Valor Añadido, o cuando se reduce artificialmente la base imponible del Impuesto sobre Sociedades mediante la llevanza de doble contabilidad, concurre igualmente el tipo del artículo 305.1 del Código Penal. En estos últimos supuestos, si además se han confeccionado libros contables ficticios, resulta de aplicación concurrente el artículo 310 del Código Penal, que sanciona específicamente los delitos contables. Una vez consumado el delito fiscal, la conversión posterior de los fondos defraudados a *bitcoin* u otros criptoactivos orientados a garantizar la privacidad, con el objetivo de ocultar las rentas o el patrimonio ilícitamente obtenido, configura un delito de autoblanqueo de capitales conforme al artículo 301.1 del Código Penal. Esta conducta se distingue del delito fiscal originario por perseguir no ya la defraudación tributaria en sí, sino la ocultación de los efectos derivados de aquella.

(78) Como hemos estudiado ya, también puede servir para ocultar el origen ilícito de recursos o encubrir rentas y activos derivados de un delito fiscal

bitcoin con cupones no genera por sí un delito fiscal –no hay tributo devengado en ese acto–, pero es parte de un *iter criminis* si la intención es iniciar una cadena de opacidad que concluya en fraude. Así, un empresario que desvía ingresos en efectivo de su negocio, los convierte en bitcoin anónimo y así no los contabiliza ni tributa por ellos, estaría cometiendo delito fiscal (79). Los delitos fiscales conllevan penas de prisión de 1 a 5 años (80) y multa del tanto al séxtuplo.

En cuanto al marco punitivo, el tipo base del artículo 305.1 del Código Penal establece una pena de prisión de uno a cinco años y multa del tanto al séxtuplo de la cuota defraudada. No obstante, concurren modalidades agravadas conforme a lo dispuesto en el párrafo segundo del artículo 305.1 y en el artículo 305.2 del mismo cuerpo legal cuando, entre otras circunstancias, la cuantía defraudada excede de seiscientos mil euros, se emplean personas o entidades interpuestas, se utilizan territorios calificados como paraísos fiscales o la conducta se desarrolla mediante organización criminal o presenta especial complejidad técnica. El ordenamiento penal prevé, asimismo, una cláusula de salida mediante la institución de la regularización tributaria. Conforme al artículo 305.4 del Código Penal, la regularización completa y veraz efectuada con anterioridad a la iniciación de actuaciones por parte de la Administración Tributaria extingue la responsabilidad penal. Si la regularización se produce con posterioridad al inicio de dichas actuaciones, el contribuyente puede beneficiarse de la aplicación de la circunstancia atenuante de reparación del daño prevista en el artículo 21.5 del Código Penal, si bien en este caso no opera la exención completa de responsabilidad (81).

---

previamente consumado, configurándose así, como una conducta de autoblanqueo de capitales según lo previsto en el artículo 301.1 del Código Penal. Finalmente, la conversión de activos a criptomonedas puede perseguir la frustración de la ejecución de deudas ya exigibles mediante el trasvase patrimonial, constituyendo en tal caso un delito de alzamiento de bienes tipificado en el artículo 257 del Código Penal.

(79) Y posiblemente blanqueo, por ser dinero de un delito fiscal, con la mencionada consideración de la directiva AML penal.

(80) Agravado hasta seis si la cuantía sobrepasa los seiscientos mil euros.

(81) Cabe añadir que la jurisprudencia del Tribunal Supremo ha interpretado esta cláusula de forma restrictiva, exigiendo que la regularización sea espontánea, íntegra y previa a cualquier requerimiento administrativo. En este sentido, la STS 1235/2021, de 17 de marzo, dictada por la Sala Segunda del Tribunal Supremo, constituye un pronunciamiento relevante en la interpretación del delito contra la Hacienda Pública previsto en el artículo 305 del Código Penal. En esta resolución, el Alto Tribunal aborda el alcance de la regularización tributaria y su incidencia sobre la existencia del delito, especialmente en relación con la presentación de autoliquidaciones por parte del contribuyente. La sentencia establece de forma clara que la mera presentación de autoliquidaciones no excluye por sí sola la

Hay que poner en relación el artículo 310 CP, que tipifica como delito la obstrucción a la labor inspectora de la Administración, lo que puede concurrir como delito conexo en casos de ocultación activa de información tributaria, especialmente cuando se emplean estructuras opacas o criptoactivos sin trazabilidad.

Cabe mencionar también el delito de alzamiento de bienes (artículo 257 CP), que se comete cuando alguien oculta o sustrae sus bienes para evitar atender responsabilidades económicas. Convertir todo el patrimonio en bitcoin y alegar insolvencia podría calificarse de alzamiento si hay voluntad de frustrar la acción de cobro de Hacienda o de otra administración. Por analogía, la jurisprudencia ha perseguido a quienes vacían cuentas y esconden dinero para no pagar multas o sanciones. Si bien el alzamiento suele requerir un acto concluyente de frustración de un embargo o ejecución, la transferencia de activos a criptomonedas en paraísos digitales podría ser vista como tal acto (82).

Por último, mencionar que, si se tratase de fondos procedentes de subvenciones o ayudas, la evasión sería delito de fraude de subvenciones del artículo 308 CP, si superase ciento veinte mil euros.

---

existencia de defraudación tributaria, si concurren otros elementos que acreditan el dolo del sujeto activo. Es decir, el hecho de que el contribuyente haya presentado declaraciones o autoliquidaciones no implica automáticamente que haya actuado de buena fe, ni que se haya excluido la voluntad defraudatoria. El Tribunal subraya que debe valorarse el conjunto de circunstancias del caso, incluyendo la ocultación de ingresos, la utilización de estructuras opacas, la simulación de operaciones o la falta de veracidad en los datos declarados. Este criterio jurisprudencial refuerza la tesis de que la regularización tributaria solo puede operar como excusa absolutoria (artículo 305.4 CP) cuando se realiza de forma completa, veraz y espontánea, y antes del inicio de actuaciones administrativas. Si la regularización se produce una vez iniciadas dichas actuaciones, puede dar lugar a la atenuante de reparación del daño (artículo 21.5 CP), pero no extingue la responsabilidad penal. En este contexto, la presentación de autoliquidaciones incompletas, tardías o estratégicamente orientadas a evitar la sanción penal puede ser considerada como insuficiente para excluir el dolo, especialmente si se demuestra que el contribuyente tenía conocimiento del fraude y actuó con intención de eludir el pago de tributos. Este enfoque ha sido reiterado por el Tribunal Supremo en otras resoluciones, consolidando una doctrina que prioriza la veracidad y la espontaneidad sobre la mera formalidad de la declaración tributaria.

(82) En relación con esta figura, Navarro Cardoso ha destacado que el carácter pseudoanónimo del bitcóin y la dificultad para trazar el origen de los fondos pueden encajar plenamente en el tipo penal de blanqueo, al permitir ocultar la procedencia ilícita mediante mecanismos digitales que fragmentan el rastro económico. El autor subraya que la criptomoneda «ha transformado el modus operandi clásico del delito económico, desdibujando los elementos clásicos del iter criminis». Navarro Cardoso, F., «Criptomonedas (en especial, bitcóin) y blanqueo de dinero», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 21-14, 2019, pp. 1-45.

Verbigracia, cuando se recibe una subvención pública y en vez de aplicarla la convierte en bitcoin para desviar su uso, defraudando su finalidad.

3. **Delitos por uso fraudulento de medios de pago**

Existen figuras penales que podrían activarse colateralmente. La LO 11/2022, en transposición de la Directiva 2019/713, reformó el CP para tipificar el uso ilícito de tarjetas, cheques de viaje u otros instrumentos de pago distintos del efectivo (83). Si alguien utiliza tarjetas de crédito robadas o datos de pago ajenos para comprar cupones de bitcoin en línea (84), podría cometer estafa informática o fraude en medios de pago. Esto no es inherente al medio no rastreable, pero es una modalidad delictiva: comprar criptoactivos con tarjetas robadas para rápidamente obtener un valor difícil de rastrear. La policía ha investigado casos así dentro del cibercrimen.

Asimismo, la falsificación de cupones o tarjetas sería otro delito: falsificar un *voucher* prepagado para intentar canjearlo podría encajar en falsedad en documento mercantil o en estafa, según el caso. También, si se organiza la venta de cupones fraudulentos (*scams*) se incurriría en delitos de estafa masiva.

4. **Infracciones administrativas y tributarias**

No todos los incumplimientos conllevan delito; de hecho, la mayoría son infracciones administrativas sancionables con multas. En materia tributaria, si la cuota defraudada no supera ciento veinte mil euros, la conducta de no declarar ganancias de criptoactivos o no declarar bienes en el extranjero se queda en infracción. De este modo, una persona que omitió declarar diez mil euros de ganancia por venta de bitcoin será sancionada con multa del cincuenta al ciento cincuenta por ciento de la cuota defraudada (85). Si además se detecta que usó mecanismos fraudulentos (86), la infracción puede calificarse de grave o muy grave.

Una infracción específica introducida por Ley 11/2021 es la de no presentar en plazo las declaraciones informativas de

(83) Artículo 248 y siguientes en relación con estafas informáticas.

(84) Algunos sitios web vendían *vouchers* de cripto pagables con tarjeta.

(85) Artículo 191 LGT, según haya o no requerimiento previo.

(86) Ad exemplum: documentos falsos, testaferros para que realicen la técnica del «pitufeo».

criptomonedas. La normativa prevé multas fijas por dato omitido o erróneo. Originalmente se barajaban sanciones durísimas (87), pero tras la sentencia del TJUE, se redujeron: actualmente la sanción por no presentar el 721 es de ciento cincuenta euros por dato con un mínimo de diez mil euros, o doscientos cincuenta euros por dato si es requerimiento, con mínimo de quince mil euros. No obstante, sigue siendo sustancial. Esto es algo a tener en cuenta: si un contribuyente compra bitcoin en el extranjero de forma anónima y no informa, afronta esta posible multa si Hacienda lo descubre –por intercambio de información internacional u otra vía–.

Otra infracción aplicable sería la de resistencia o negativa a requerimientos de información de la AEAT o SEPBLAC. Si un sujeto obligado, verbigracia un *exchange* se niega a identificar a un cliente alegando protección de datos, incurrirá en sanciones muy graves en el régimen PBC (88). Y un particular que ignore un requerimiento de Hacienda para aclarar el origen de unos fondos puede ser multado por desobediencia a la LGT.

IX. DERECHO A LA INTIMIDAD, PROTECCIÓN DE DATOS PERSONALES Y OPERACIONES CON CUPONES SOBRE CRIPTOACTIVOS

La cuestión del anonimato es importante en el tema que nos ocupa, pues la motivación para utilizar medios de pago no rastreables es justamente proteger la identidad y el rastro financiero del adquirente de bitcoin. Sin embargo, este legítimo deseo de confidencialidad conflige con imperativos de seguridad jurídica y pública, en particular la prevención de delitos. En este epígrafe analizamos el delicado equilibrio entre el anonimato y la necesidad de trazabilidad, así como aspectos de ciberseguridad inherentes al uso de criptomonedas de forma anónima.

En España no existe un derecho absoluto al anonimato en las transacciones financieras. Si bien la normativa de protección de datos (RGPD) resguarda la información personal, las leyes antiblanqueo establecen excepciones claras: los sujetos obligados deben identificar clientes y conservar sus datos durante al menos diez años (Ley 10/2010, artículo 25), incluso sin el consentimiento del interesado, por mandato

(87) Eran cinco mil euros por dato omitido.
(88) Multas millonarias posibles y hasta revocación de licencia

legal (89). Además, aunque el RGPD exige consentimiento para el tratamiento de datos, contempla excepciones cuando el tratamiento es necesario para cumplir una obligación legal (artículo 6.1.c RGPD). La normativa española se alinea con esta excepción. Desde una perspectiva constitucional, el derecho al secreto de las comunicaciones financieras o al anonimato no está reconocido; más bien, la Ley puede imponer deberes de información por razones de interés general –lucha contra el delito, fraude fiscal–. Por tanto, la persona que pretende permanecer en la sombra utilizando efectivo y cupones puede estar contraviniendo obligaciones legales si ello implica no atender requerimientos de información –por ejemplo, no presentar el Modelo 721 o mentir a Hacienda sobre el origen de fondos– (90).

No obstante, el anonimato en las transacciones es valorado legítimamente por muchos usuarios de criptomonedas no para delinquir, sino por filosofía –desconfianza hacia el sistema bancario, deseo de autonomía– o para protegerse de eventual inseguridad –por ejemplo, en países con inestabilidad–. En España el anonimato se debe conjugar con la ley: es posible mantener reserva sobre ciertas transacciones, pero siempre con el límite de cumplir las normas. Por ejemplo, un ciudadano puede comprar bitcoin con varios cupones de cien euros sin registrarse y eso puede quedar en la práctica limitado; sin embargo, si esos bitcoines generaran luego ganancias, deberá declararlas, revelando indirectamente la tenencia.

Las empresas que verifican la identidad de los compradores de cupones manejan datos personales sensibles –documentos de identidad, importes comprados, direcciones de criptomoneda–. Estas están sujetas al RGPD y a la Ley Orgánica 3/2018 (LOPDGDD), debiendo tomar medidas para proteger esa información. Un riesgo colateral de la compra «semi-anónima» es que, si el usuario confía en un proveedor poco conocido, sus datos o sus fondos podrían ser comprometidos. Ha habido casos de *exchanges* no regulados que simplemente desaparecieron con los fondos de clientes o de filtraciones

(89) En efecto, el anonimato financiero no está reconocido como derecho fundamental en el ordenamiento jurídico español. La protección de datos (artículo 18.4 CE y RGPD) no ampara el anonimato frente a obligaciones legales de identificación, especialmente en el ámbito financiero.

(90) El Tribunal Constitucional ha admitido que ciertos límites al derecho a la intimidad y a la protección de datos son legítimos si están previstos por ley, persiguen fines constitucionalmente legítimos y son proporcionados. En este caso, la trazabilidad financiera se considera esencial para combatir delitos económicos complejos. Este es el argumento dado en la STC 292/2000, de 30 de noviembre, FJ 7 (y ss.), sobre la legitimidad de la cesión de datos tributarios en el marco de la investigación penal.

de datos de usuarios cripto en manos de *hackers*, lo que puede exponer a los titulares a ataques de *phishing* o incluso amenazas físicas.

El anonimato en la adquisición de bitcoin es un arma de doble filo: por un lado, protege al individuo de la exposición de su patrimonio y decisiones –lo cual en general es deseable bajo el prisma de libertades individuales–, pero, por otro lado, puede facilitar actividades ilegales y, aun en usos legítimos, acarrea riesgos –falta de respaldo si algo sale mal, auto-responsabilidad en seguridad–. La legislación actual apuesta claramente por sacrificar parte del anonimato en favor de la seguridad colectiva: las tendencias –MiCA, Travel Rule, registros de usuarios– indican que el espacio para la adquisición realmente anónima se reducirá drásticamente. Solo quedarán nichos fuera de la ley –como los mercados negros en la *darkweb*–, cuyo uso ya implicará de por sí un riesgo penal.

Desde la perspectiva del usuario responsable, la recomendación es equilibrar anonimato y cumplimiento: puede tomar medidas como usar *wallets* propios en lugar de dejar cripto en *exchanges* –lo que mejora anonimato y seguridad de custodia–, pero no debe eludir sus obligaciones fiscales ni legales. Asimismo, es prudente diversificar la exposición de datos: por ejemplo, puede comprar un poco en distintos servicios para no concentrar toda su información en un solo proveedor –limitando daño en caso de brecha de datos–, siempre sin incurrir en fraccionamiento sospechoso. Finalmente, debe mantenerse informado sobre las mejores prácticas de seguridad –2FA, almacenamiento en frío, *backups*– para que la búsqueda de anonimato no termine en pérdida de sus activos por descuido.

X. CONSIDERACIONES FINALES

Primera

La posibilidad técnica de adquirir *bitcoin* mediante cupones prepagados y otros medios de pago no rastreables no solo es real, sino que resulta cada vez más accesible al público general, evidenciando una demanda creciente de anonimato en las transacciones financieras. Sin embargo, esta operativa se desarrolla en un entorno jurídico en constante evolución que, tanto en el ordenamiento español como a nivel de la Unión Europea, se orienta decididamente hacia la trazabilidad y la transparencia financiera como principios rectores. Lo que en un primer momento pudo percibirse como un vacío o laguna legal que permitía la compra de criptoactivos al margen del ordenamiento jurídico está siendo progresivamente integrado

mediante la entrada en vigor de nueva normativa específica, en especial en el ámbito de la prevención del blanqueo de capitales y la supervisión de los proveedores de servicios de criptoactivos.

Segunda

En el ordenamiento jurídico español, *bitcoin* no se reconoce como moneda de curso legal, sino que se le atribuye la naturaleza de un bien mueble inmaterial, susceptible de propiedad y tráfico lícito. En consecuencia, su compraventa es una actividad legal en España, pero debe observar tanto las reglas generales aplicables a cualquier negocio jurídico como la normativa específica. El Tribunal Supremo, en una sentencia de 2019, contribuyó a perfilar esta calificación jurídica, mientras que en el plano comunitario la Unión Europea, mediante sucesivas Directivas y Reglamentos –sobre todo en sede de blanqueo, aunque el nuevo Reglamento de Mercados de Criptoactivos (MiCA) nos ofrece una regulación de ordenación de sector «industrial»–, ha sentado las bases de un marco regulador unificado que integra a los criptoactivos y a sus proveedores dentro de la legalidad financiera ordinaria, equiparándolos en lo esencial a otros instrumentos y agentes del sistema financiero.

Tercera

Los medios de pago no rastreables –*v.gr.*, los *vouchers* o cupones anónimos–, tradicionalmente asociados a la economía sumergida, se encuentran sometidos a restricciones normativas cada vez más estrictas. La regulación actual ha impuesto umbrales de anonimato muy reducidos –actualmente, por ejemplo, apenas ciento cincuenta euros para las tarjetas prepago anónimas en virtud de la normativa antiblanqueo europea y su trasposición nacional–, junto con la prohibición de ciertos usos. En consecuencia, el margen para adquirir cantidades significativas de bitcoin de forma completamente anónima y lícita, mediante el «puente» de los *vouchers* o cupones, se ha estrechado. Además, cualquier intento de eludir estos límites mediante la fragmentación deliberada de operaciones (el denominado «smurfing» o «pitufeo») no solo genera sospechas de ilegalidad, sino que contraviene expresamente la Ley 10/2010, que prohíbe la división artificiosa de transacciones para sortear los umbrales de diligencia debida, exponiendo al agente a eventuales responsabilidades legales por indicios de blanqueo.

Una vez dentro de internet y del *blockchain* la cosa cambia y se refuerza el control. Entre proveedores de servicios de criptoactivos (CASP), existe la obligación de acompañar todas las transferencias de criptoactivos con información sobre el ordenante y el beneficiario, sin establecer un umbral general de exclusión merced al Reglamento (UE) 2023/1113, si bien el artículo 16 del Reglamento introduce medidas reforzadas cuando las transferencias implican carteras autocustodiadas –self-hosted wallets–. En estos casos, el proveedor debe verificar la identidad del titular de la *wallet* fría si la transferencia supera los mil euros, pero este umbral solo aplica a esa situación específica, no como regla general. A diferencia de la Quinta Directiva AML (UE) 2018/843, que sí contemplaba umbrales de anonimato –ciento cincuenta para tarjetas prepago físicas y cincuenta euros para remotas–, el Reglamento 2023/1113 elimina tales umbrales para las transferencias de criptoactivos entre CASP.

Cuarta

Si bien el empleo de cupones prepagados adquiridos en efectivo permite eludir el registro bancario directo –dejando al comprador en apariencia fuera del radar de los intermediarios financieros tradicionales–, siempre subsiste algún rastro de la transacción, ya sea en la plataforma cripto utilizada para el canje del cupón o en la propia cadena de bloques pública, susceptible de ser analizado *a posteriori*. En la práctica, por tanto, el anonimato nunca es absoluto: la combinación de potentes herramientas de analítica de datos con las obligaciones legales de transparencia termina por vincular las distintas piezas tarde o temprano. Un comprador que inicialmente cree mantenerse en el anonimato por haber empleado efectivo puede, con el tiempo, ser identificado a través de su interacción con *exchanges* regulados (sujetos a la *travel rule* y a realizar suministro de información obligatorio de operaciones sospechosas), mediante los modelos informativos fiscales que revelan tenencias u operaciones con criptoactivos, o incluso en el marco de investigaciones policiales que logren enlazar la información on-chain con datos personales obtenidos de proveedores obligados.

Quinta

El ordenamiento, tanto español como europeo, impone múltiples capas de control sobre la operativa de adquisición anónima de

criptoactivos. En primer lugar, la normativa de prevención del blanqueo de capitales obliga a las plataformas de criptomonedas y demás sujetos obligados a aplicar diligencia debida con sus clientes (*Know Your Customer* o KYC) e informar de actividades inusuales o sospechosas a las autoridades competentes. En segundo lugar, el Derecho penal sanciona con severidad el blanqueo de capitales, incluyendo expresamente el realizado mediante criptoactivos, equiparándolo en gravedad al blanqueo tradicional (artículo 301 y ss. del Código Penal), y prevé agravantes cuando median profesionales o entidades obligadas que facilitan dichas operaciones ilícitas. En tercer lugar, la normativa fiscal exige declarar las rentas y patrimonios en criptomonedas del mismo modo que cualquier otro activo, habiéndose introducido nuevos formularios informativos específicos (modelos 172, 173 y 721, entre otros) para aflorar estos bienes ante la Hacienda Pública. Por último, a nivel de la Unión Europea, mediante directivas y reglamentos recientes, se está armonizando este conjunto de obligaciones en todos los Estados miembros, eliminando así posibles puntos ciegos o lagunas de regulación: ningún país de la UE puede erigirse ya en un refugio normativo, pues todos deben tipificar y perseguir el blanqueo de capitales de forma homogénea y aplicar controles equivalentes sobre los operadores de criptoactivos.

Sexta

En el plano penal, la compraventa anónima de bitcoin se erige en un medio propicio para el blanqueo de capitales ilícitos, motivo por el cual se halla bajo un escrutinio especial. El legislador español ha reforzado la respuesta punitiva frente a estas conductas: el delito de blanqueo de capitales (artículo 301 CP) se castiga con penas elevadas y, en línea con las exigencias europeas (*v.gr.*, Directiva (UE) 2018/1673), se prevén agravantes específicas cuando intervienen sujetos obligados del sector financiero o de criptoactivos que actúan como cómplices o facilitadores, evidenciando una intolerancia absoluta hacia la connivencia de intermediarios. Del mismo modo, el fraude fiscal a gran escala valiéndose de criptomonedas no queda impune: superar los umbrales establecidos configura un delito contra la Hacienda Pública, sin que la naturaleza digital del medio de pago exima de responsabilidad penal. En definitiva, los criptoactivos no constituyen un refugio seguro para delincuentes; por el contrario, se les aplica el rigor de la ley con la misma severidad que si emplearan métodos tradicionales de blanqueo, adaptándose las herramientas investigativas –como el análisis forense de la blockchain, la

cooperación internacional o los requerimientos de información a *exchanges*– para afrontar eficazmente estos nuevos desafíos tecnológicos.

Séptima

En el ámbito tributario, la Agencia Tributaria española ha situado a las criptomonedas entre sus objetivos prioritarios, tal como reflejan sus planes anuales de control más recientes y la introducción de obligaciones informativas específicas. Los contribuyentes deben asumir que Hacienda, directa o indirectamente, llegará a conocer sus tenencias y operaciones en criptoactivos, ya sea mediante los datos aportados por terceros obligados (por ejemplo, *exchanges* que informan de las operaciones de sus clientes mediante el modelo 172) o a través de los deberes de información de los propios contribuyentes (como el modelo 721 para declarar criptoactivos en el extranjero, incorporado por la Ley 11/2021). En caso de detectarse incumplimientos, la Administración Tributaria impondrá sanciones contundentes conforme a la Ley General Tributaria, sin perjuicio de eventuales derivaciones penales si la cuantía defraudada supera los umbrales del delito fiscal. Cabe destacar que, tras ciertas vacilaciones iniciales, hoy existe una claridad normativa considerable sobre el tratamiento fiscal de la mayoría de operaciones con criptomonedas: las ganancias patrimoniales derivadas de su enajenación tributan en el IRPF del mismo modo que las obtenidas con activos tradicionales; los intercambios de criptomoneda por moneda fiduciaria están exentos de IVA (conforme a la jurisprudencia del TJUE desde el caso Hedqvist de 2015, que equiparó estas transacciones a las operaciones financieras con divisas); y los criptoactivos se incluyen en la base del Impuesto sobre el Patrimonio –cuando dicho impuesto resulta de aplicación– al igual que cualquier otro bien. Esta definición legal precisa elimina las posibles excusas de desconocimiento e impele a los contribuyentes a cumplir escrupulosamente con sus obligaciones fiscales en materia de criptoactivos.

Octava

En materia de derecho a la intimidad y protección de datos personales, la búsqueda de un anonimato absoluto en las transacciones con bitcoin se revela no solo inviable, sino incluso peligrosa para el propio usuario; en contraste, un individuo precavido

puede mantener un nivel razonable de pseudoanonimato sin apartarse del marco legal vigente. El ordenamiento jurídico, a través de las normas de protección de datos personales y de excepciones justificadas por la prevención del delito, no pretende eliminar el anonimato legítimo de los particulares, sino evitar su abuso con fines ilícitos; sin embargo, la frontera entre el ejercicio legítimo del derecho a la intimidad financiera y la ocultación maliciosa de actividades es difusa y queda abierta a interpretación. Lo cierto es que la evolución normativa reciente se inclina claramente a favor de la seguridad pública y la trazabilidad: iniciativas legislativas tanto nacionales como europeas (por ejemplo, la ampliación de las obligaciones de identificación de usuarios en el sector cripto y la aplicación de la «travel rule») están reduciendo drásticamente los espacios para el anonimato efectivo en las operaciones con criptoactivos. Queda en el plano del debate ético y de los derechos fundamentales la cuestión de si debería preservarse un margen de anonimato para pequeñas transacciones inocuas –un debate análogo al relativo al uso del dinero en efectivo–, pero por el momento la postura del legislador ha sido la de circunscribir ese margen a lo estrictamente necesario y someter incluso esas transacciones mínimas a una estrecha supervisión.

Novena

Las tipologías delictivas asociadas al uso opaco de criptomonedas son variadas, pero comparten un elemento común: la utilización fraudulenta de estos instrumentos para fines ilícitos. En primer término, sobresale el delito de blanqueo de capitales, pues la opacidad que ofrece el ecosistema cripto puede ser explotada para introducir en el circuito legal fondos de procedencia ilícita (artículo 301 CP), riesgo que ha motivado las especiales cautelas normativas ya mencionadas. Junto a ello, se perfilan los delitos contra la Hacienda Pública cuando se emplean criptoactivos para evadir impuestos a gran escala (artículo 305 CP, punible a partir de una cuota defraudada superior a ciento veinte mil euros anuales); el alzamiento de bienes si se utilizan criptomonedas para sustraer patrimonios de la acción de acreedores o del Fisco (artículo 257 CP); así como posibles estafas vinculadas al uso fraudulento de medios de pago tradicionales en la adquisición de cupones o tarjetas. Es imperativo que tanto los particulares como las empresas conozcan estos riesgos penales y actúen con la debida diligencia para no incurrir –ni siquiera por imprudencia– en conductas que pudieran

encuadrarse en alguna de estas figuras delictivas. En particular, las empresas que operan en el sector de criptoactivos se arriesgan no solo a sanciones administrativas gravísimas (multas millonarias y posibles revocaciones de licencias), sino también a la eventual responsabilidad penal de la persona jurídica conforme al Código Penal si incumplen de forma grave sus obligaciones de prevención; los individuos, por su parte, se exponen a la privación de libertad y a severas consecuencias patrimoniales cuando traspasan los umbrales que separan la mera infracción administrativa del delito.

Décima

Es factible conjugar el uso innovador de las criptomonedas con el pleno respeto a la legalidad, sin tener que renunciar por completo a ciertas cotas de anonimato o privacidad por parte del usuario. En la práctica, es viable emplear criptoactivos y preservar hasta cierto punto el anonimato, pero siempre dentro de los cauces normativos: ello implica cumplir con las obligaciones de registro y autorización cuando la actividad lo requiera, declarar los rendimientos y tenencias de criptoactivos en los tributos correspondientes, y aceptar los mecanismos de supervisión e información impuestos por las autoridades financieras. Atrás van quedando los tiempos en que el ecosistema «cripto» operaba al margen del ordenamiento como un «lejano oeste» sin ley; en la actualidad, estos activos se han incorporado plenamente al sistema financiero, y los sujetos que actúan en este ámbito –sean empresas o usuarios particulares– deben comportarse con la misma responsabilidad, transparencia y diligencia debida que se exige tradicionalmente a los operadores del sector bancario. Este proceso de normalización regulatoria, propiciado tanto por iniciativas europeas como por desarrollos internos, ha supuesto someter a las criptomonedas y a sus intermediarios a estándares equivalentes a los de los demás instrumentos financieros, con el objetivo de garantizar la estabilidad de los mercados y la confianza del público en este nuevo ecosistema digital.

Corolario

¿Es bueno que los ciudadanos tengan un pequeño margen de anonimato? Actualmente, en las tarjetas prepago lo encontramos en los 150 euros (50 euros en adquisiciones telemáticas) y puede ser

una buena opción dejar esa puerta abierta sin tratar a todos sus usuarios como criminales. Mientras tanto, se pueden centrar los esfuerzos en las grandes operaciones de blanqueo o defraudación. Este equilibrio mantiene el derecho a un mínimo de anonimato financiero a la par que se combaten las operaciones de blanqueo serias. Ahora bien, algunos usuarios podrían pensar en dividir una compra grande de bitcoin en pequeñas porciones para evitar controles. Esta práctica, además de potencialmente constituir indicio de blanqueo, puede ser detectada y ser considerada un todo. La Ley 10/2010 prohíbe la fragmentación artificiosa de operaciones para evitar umbrales de diligencia debida. Por tanto, es aconsejable actuar con transparencia: si se van a comprar cantidades significativas, es preferible pasar por los procedimientos de identificación de una vez, en lugar de arriesgarse a incurrir en sospecha de haber creado una estructura infractora. Reiteramos que es legítimo querer un cierto anonimato; pero para ello, en lugar de recurrir a ilegalidades, el usuario puede tomar medidas: usar monederos «fríos», rotar direcciones para que su historial *on-chain* no sea fácilmente asociable a una única identidad o usar VPNs y redes cifradas (Tor) al realizar transacciones en línea, todo lo cual es legal. Lo que se debe evitar son herramientas expresamente prohibidas o sospechosas. Si se emplean técnicas de anonimato avanzadas –por ejemplo, *atomic swaps* y *zero-knowledge proofs*–, se debe estar consciente de que pueden levantar alertas.

XI. BIBLIOGRAFÍA

Doctrina

Capaccioli, S.: «Vat & Bitcoin»: *EC Tax Review*, vol. 23, n.º 6, 2014, pp. 361-362.

Casals Fernández, Á.: «Las criptomonedas frente al delito de blanqueo de capitales y la financiación del terrorismo», *Anuario de Derecho Penal y Ciencias Penales*, vol. LXXV, 2022.

Custers, B.; Oerlemans, J.-J.; Pool, R.: «Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies», *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 28, n.º 2, 2020, pp. 121-152.

Díaz Bernardos, A.: «Explorando las huellas digitales de los criptoactivos mediante fuentes abiertas», *Ciencia Policial*, n.º 182, 2024, pp. 271-311. Disponible en: https://revistas.usal.es/cuatro/index.php/2254-0326/article/view/31816 [consulta: 15 de octubre de 2025].

Ehrke Rabel, T. y Zechner, L.: «VAT Treatment of Cryptocurrency Intermediation Services», *Intertax*, vol. 48, n.º 5, 2020, pp. 498-514.

Fetsyak Senkiv, I.: «Consideraciones sobre la prevención del blanqueo de capitales y financiación del terrorismo mediante los tokens no fungibles (NFT)», *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, n.º 20, 2022, pp. 91-103. DOI: https://doi.org/10.18172/redur.5599 [consulta: 15 de octubre de 2025].

Foley, S.; Karlsen, J. R.; Putniņš, T. J.: «Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?», The Review of Financial Studies, vol. 32, n.º 5, 2019, pp. 1798-1853, DOI: 10.1093/rfs/hhz015 [consulta: 15 de octubre de 2025]

Jucan Sicignano, G.: «L'acquisto di bitcoin con denaro di provenienza illecita», *Archivio penale*, n.º 2, 2020. Disponible en: https://archiviopenale.it/File/DownloadArticolo?codice=2986a7e7-4359-4b5a-a84b-df9a71f580c6&idarticolo=24907 [consulta: 15 de octubre de 2025].

López Martínez, M.: Situación de la regulación de la prevención del blanqueo de capitales y de la financiación del terrorismo en el marco de los criptoactivos, *Instituto de Estudios Financieros*, 2023. [Consultado el 15 de octubre de 2025]. Disponible en: https://www.iefweb.org/publicacio_odf/situacion-de-la-regulacion-de-la-prevencion-del-blanqueo-de-capitales-y-de-la-financiacion-del-terrorismo-en-el-marco-de-los-criptoactivos/

Miras Marín, N.: «El régimen jurídico-tributario del bitcóin», Estudios financieros. Revista de contabilidad y tributación: Comentarios, casos prácticos, n.º 406, 2017, pp. 101-136.

— «La determinación de la naturaleza jurídica del bitcoin a la luz de la reciente sentencia 326/2019 del Tribunal Supremo», Revista Aranzadi de derecho y nuevas tecnologías, n.º 51, 2019.

Montesinos Oltra, S.: «La pragmática incoherencia de la calificación de las criptomonedas a efectos tributarios», *Crónica Tributaria*, n.º 183, 2022, pp. 101-136.

Muñoz Marín, A.: «Blanqueo de capitales en los supuestos de tráfico de drogas por el mismo sujeto: el autoblanqueo y el principio non bis in ídem», *CEFLegal: Revista práctica de derecho. Comentarios y casos prácticos*, n.º 162, 2014, pp. 212-216.

Navarro Cardoso, F.: «Criptomonedas (en especial, bitcóin) y blanqueo de dinero», *Revista Electrónica de Ciencia Penal y Criminología*, n.º 21, 2019. Disponible en: https://revistacriminologia.com/21/recpc21-14.pdf [consulta: 15 de octubre de 2025].

Navas Blánquez, J. J.: El embargo y decomiso de criptomonedas en el Espacio Judicial Europeo. *Revista de Estudios Europeos*, [S. l.], n. Monográfico 1, p. 349-383, 2023. DOI: 10.24197/ree. Monográfico 1.2023.349-383. Disponible en: https://revistas.uva.es/index.php/ree/article/view/7402. [Consulta: 15 de octubre de 2025].

Ness, S.: «VAT/GST Harmonisation Challenges for Digital Assets such as Bitcoin and NFTs in the EU (following C-264/14 Hedqvist)», Journal of Business Economics and Management, 2024.
Nieto Montero, J. J.: «Monedas virtuales en la Directiva 2018/843, su tributación y blanqueo», en *X Congreso Internacional sobre prevención y represión del blanqueo de dinero y IV Congreso de la Asociación Iberoamericana de Derecho penal económico y de la empresa: Ponencias y conclusiones del congreso. El blanqueo en la Unión Europea, su incidencia en el mundo digital y la internacionalización del Derecho penal,* celebrado en la Facultad de Derecho de la Universidad de Santiago de Compostela, en julio de 2024, València: Tirant lo Blanch, 2025, 2025, pp. 623-624.
Pérez López, X.: «Las criptomonedas: consideraciones generales y empleo con fines de blanqueo», en Fernández Bermejo (Dir.), *Blanqueo de capitales y TIC: Marco jurídico europeo, modus operandi y criptomonedas,* Thomson-Reuters Aranzadi, Cizur Menor, 2019, p. 87.
Tanyushcheva, N.: «Parámetros cuantitativos de la regulación antiblanqueo de capitales», *Análisis Financiero: Ciencia y Experiencia*, vol. 25, n.º 4, 2020, DOI: 10.24891/df.25.4.416 [consulta: 15 de octubre de 2025]
Wang, J.: «A Simplified Tax Regime for Taxing Cryptocurrencies», *Intertax*, vol. 53, n.º 3, 2025, pp. 245-266.

XII. JURISPRUDENCIA Y RESOLUCIONES

Dirección General de Tributos, Consulta V0808-20.
Dirección General de Tributos, Consulta Vinculante V1604-18.
Dirección General de Tributos, Consultas V0999-18 y V1481-18.
SAP Asturias (Sección 1.ª) núm. 37/2015, de 30 de abril.
STJUE de 22 de octubre de 2015, asunto C-264/14 (Skatteverket v. Hedqvist).
STJUE de 27 de enero de 2022, asunto C-788/19 (Comisión vs. España).
STS (Sala Penal) 2109/2019, de 20 de junio.
STS (Sala Penal) núm. 326/2019, de 20 de junio.
STS 277/2018, de 8 de junio (Sala Penal).
STS 4217/2018, de 13 de diciembre (Sala Penal).

Informes

FATF – GAFI, *«Virtual Assets Red Flag Indicators of ML/TF»*, Sept. 2020.
SEPBLAC (Servicio Ejecutivo PBC), *«Guía de prácticas en materia de prevención del blanqueo con criptomonedas»*, 2021.